PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-260803
(43)Date of publication of application : 16.09.2004

(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 12/28
H04Q 7/38

(21)Application number : 2004-015193 (71)Applicant : SONY CORP
(22)Date of filing : 23.01.2004 (72)Inventor : SUZUKI HIDEYUKI

(30)Priority
Priority number : 2003026544 Priority date : 03.02.2003 Priority country : JP

(54) RADIO AD HOC COMMUNICATION SYSTEM, TERMINAL, ATTRIBUTE CERTIFICATE ISSUE PROPOSING AND REQUESTING METHOD AT TERMINAL, AND PROGRAM FOR IMPLEMENTATION THEREOF

(57)Abstract:
PROBLEM TO BE SOLVED: To autonomously carry out the issue of an attribute certificate in a distributed radio ad hoc communication system.
SOLUTION: A terminal B200 transmits a beacon 2011 to log on a network of a radio ad hoc communication system. In the beacon 2011, whether the terminal B200 has an attribute certificate or not is indicated. A terminal A100 which has received the beacon 2011 checks the beacon. When it is determined that the terminal B200 does not have the attribute certificate, the terminal A100 transmits an attribute certificate issue proposing message 1032 to the terminal B200 for requesting the issue of an attribute certificate. In response to this, the terminal B200 transmits an attribute certificate issue requesting message 2041. Then, the terminal A100 transmits an attribute certificate issuing message 1052 to the terminal B200.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1]

It is the wireless ad hoc communication system constituted with two or more terminals,

The 1st terminal which transmits a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,

The 2nd terminal it is proposed to said 1st terminal that said signal is answered and carries out a terminal authority authentication certificate issue request

Wireless ad hoc communication system to provide.

[Claim 2]

A receiving means to receive a signal including beacon information,

reception of the signal with which this receiving means includes predetermined beacon information from other terminals carries out a terminal authority authentication certificate issue request -- as -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal

The terminal characterized by providing.

[Claim 3]

A means to acquire the terminal identification information on the terminal of these

these others from said signal from a terminal besides the above which said receiving means received is provided further,
Said terminal authority authentication certificate issue proposal means performs said proposal based on said terminal identification information.
The terminal according to claim 2 characterized by things.
[Claim 4]
In case said terminal authority authentication certificate issue proposal means proposes said terminal authority authentication certificate issue request to a terminal besides the above, it presents the public key certificate of said terminal collectively.
The terminal according to claim 2 characterized by things.
[Claim 5]
A receiving means to receive a signal including beacon information,
if the signal with which this receiving means includes predetermined beacon information from other terminals is received -- being concerned -- others -- the terminal authority authentication certificate which makes a terminal an owner -- publishing -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal
The terminal characterized by providing.
[Claim 6]
A means to acquire the terminal identification information on the terminal of these these others from said signal from a terminal besides the above which said receiving means received is provided further,
Said terminal authority authentication certificate issue proposal means performs said proposal based on said terminal identification information.
The terminal according to claim 5 characterized by things.
[Claim 7]
In case said terminal authority authentication certificate issue proposal means proposes said terminal authority authentication certificate issue request to a terminal besides the above, it presents the public key certificate of said terminal collectively.
The terminal according to claim 5 characterized by things.
[Claim 8]
The receiving means for receiving a signal including beacon information,
the case where the signal with which this receiving means includes beacon information from other terminals is received -- setting -- being concerned -- others -- if said signal does not show the purport in which a terminal has a terminal authority authentication certificate, a terminal authority authentication certificate issue request is carried out -- as -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal
The terminal characterized by providing.
[Claim 9]
A means to acquire the terminal identification information on the terminal of these

these others from said signal from a terminal besides the above which said receiving means received is provided further,
Said terminal authority authentication certificate issue proposal means performs said proposal based on said terminal identification information.
The terminal according to claim 8 characterized by things.
[Claim 10]
In case said terminal authority authentication certificate issue proposal means proposes said terminal authority authentication certificate issue request to a terminal besides the above, it presents the public key certificate of said terminal collectively.
The terminal according to claim 8 characterized by things.
[Claim 11]
The terminal authority authentication certificate issue request receiving means for receiving a terminal authority authentication certificate issue request,
this terminal authority authentication certificate issue request receiving means -- said -- others -- receiving a terminal authority authentication certificate issue request from a terminal -- being concerned -- others -- the check means to which the information about a terminal is displayed and a check is urged,
A terminal authority authentication certificate issue means to notify refusal of a terminal authority authentication certificate issue request to a terminal besides the above when a terminal authority authentication certificate is published to a terminal besides the above when said check is made, and said check is refused
The terminal according to claim 10 characterized by providing in a pan.
[Claim 12]
The terminal authority authentication certificate issue terminal list table holding the public key certificate of a terminal authority authentication certificate issue terminal is provided further,
Said terminal authority authentication certificate issue means transmits the public key certificate of said terminal authority authentication certificate issue terminal held on the occasion of issue of said terminal authority authentication certificate at said terminal authority authentication certificate issue terminal list table to a terminal besides the above.
The terminal according to claim 11 characterized by things.
[Claim 13]
The terminal authority authentication certificate lapse list table holding the lapse list of terminal authority authentication certificates is provided further,
Said terminal authority authentication certificate issue means transmits said terminal authority authentication certificate lapse list held on the occasion of issue of said terminal authority authentication certificate at said terminal authority authentication certificate lapse list table to a terminal besides the above.
The terminal according to claim 11 characterized by things.
[Claim 14]

The receiving means for receiving a signal including beacon information,
the case where the signal with which this receiving means includes beacon information from other terminals is received -- setting -- being concerned -- others -- if said signal does not show the purport in which a terminal has a terminal authority authentication certificate -- being concerned -- others -- the terminal authority authentication certificate which makes a terminal an owner -- publishing -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal
The terminal characterized by providing.
[Claim 15]
A means to acquire the terminal identification information on the terminal of these these others from said signal from a terminal besides the above which said receiving means received is provided further,
Said terminal authority authentication certificate issue proposal means performs said proposal based on said terminal identification information.
The terminal according to claim 14 characterized by things.
[Claim 16]
In case said terminal authority authentication certificate issue proposal means proposes said terminal authority authentication certificate issue request to a terminal besides the above, it presents the public key certificate of said terminal collectively.
The terminal according to claim 14 characterized by things.
[Claim 17]
A transmitting means to transmit a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
A terminal authority authentication certificate issue proposal receiving means to receive the proposal of the terminal authority authentication certificate issue request to said signal,
this terminal authority authentication certificate issue proposal receiving means receives said proposal from other terminals -- being concerned -- others -- the check means to which the information about a terminal is displayed and a check is urged,
the case where said check is made -- said -- others -- the case where requested issue of a terminal authority authentication certificate to the terminal, and said check is refused -- said -- others -- a terminal authority authentication certificate issue request means to notify refusal of a terminal authority authentication certificate issue proposal to a terminal
The terminal to provide.
[Claim 18]
In case said terminal authority authentication certificate issue request means requests said terminal authority authentication certificate issue to a terminal besides the above, it presents the public key certificate of said terminal collectively.

The terminal according to claim 17 characterized by things.
[Claim 19]
A transmitting means to transmit a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
A terminal authority authentication certificate issue proposal receiving means to receive the proposal of the terminal authority authentication certificate issue request to said signal,
this terminal authority authentication certificate issue proposal receiving means receives said proposal from other terminals -- being concerned -- others -- the check means to which the information about a terminal is displayed and a check is urged,
A terminal authority authentication certificate issue request means to request issue of a terminal authority authentication certificate to a terminal besides the above when the terminal authority authentication certificate concerned is received when said proposal contains the terminal authority authentication certificate [finishing / issue], if said check is made, and said proposal does not contain the terminal authority authentication certificate [finishing / issue]
The terminal to provide.
[Claim 20]
In case said terminal authority authentication certificate issue request means requests said terminal authority authentication certificate issue to a terminal besides the above, it presents the public key certificate of said terminal collectively.
The terminal according to claim 19 characterized by things.
[Claim 21]
A receiving means to receive a signal including beacon information,
A terminal authority authentication certificate issue request means to request to a terminal besides the above to carry out terminal authority authentication certificate issue if the signal with which this receiving means includes predetermined beacon information from other terminals is received
The terminal characterized by providing.
[Claim 22]
A means to acquire the terminal identification information on the terminal of these these others from said signal from a terminal besides the above which said receiving means received is provided further,
A terminal authority authentication certificate issue request means performs said proposal based on said terminal identification information.
The terminal according to claim 21 characterized by things.
[Claim 23]
The terminal authority authentication certificate table holding the 1st terminal authority authentication certificate in which the access permission in the end of a local is shown,

The receiving means for receiving a signal including beacon information,
the case where the signal with which this receiving means includes beacon information from other terminals is received -- setting -- being concerned -- others -- the 2nd terminal-authority authentication certificate in which the access permission of a terminal is shown -- being concerned -- others -- said 1st terminal-authority authentication certificate held at said terminal-authority authentication certificate table when said signal showed the purport which a terminal has -- showing -- said -- others -- an authentication demand means require said authentication in the end of a local from a terminal
The terminal characterized by providing.
[Claim 24]
The terminal authority authentication certificate issue terminal list table holding the public key certificate of a terminal authority authentication certificate issue terminal,
An authentication demand receiving means to receive the 2nd authentication demand which answers the authentication demand by said authentication demand means, and a terminal besides the above requires,
A verification means to verify said 2nd terminal authority authentication certificate contained in said 2nd authentication demand which this authentication demand receiving means received with the public key contained in the public key certificate held at said terminal authority authentication certificate issue terminal list table
The terminal according to claim 23 characterized by providing in a pan.
[Claim 25]
The terminal authority authentication certificate lapse list table holding a terminal authority authentication certificate lapse list is provided further,
Said verification means makes a judgment with authentication failure, when said 2nd terminal authority authentication certificate is invalidated in said terminal authority authentication certificate lapse list held at said terminal authority authentication certificate lapse list table.
The terminal according to claim 24 characterized by things.
[Claim 26]
The terminal authority authentication certificate issue terminal list table holding the public key certificate of a terminal authority authentication certificate issue terminal,
A transmitting means to transmit a signal including the beacon information which shows the purport which has the 2nd terminal authority authentication certificate to other terminals which have the 1st terminal authority authentication certificate,
The terminal authority authentication certificate table holding said 2nd terminal authority authentication certificate in which the access permission in the end of a local is shown,
An authentication demand receiving means to receive the 1st authentication demand from other terminals to said signal,
A verification means to verify said 1st terminal authority authentication certificate

contained in said 1st authentication demand which this authentication demand receiving means received with the public key contained in the public key certificate held at said terminal authority authentication certificate issue terminal list table, if authentication succeeds in this verification means -- said -- others -- said 2nd terminal authority authentication certificate held to the terminal at said terminal authority authentication certificate table -- showing -- said -- others -- an authentication demand means to perform the 2nd authentication demand which requires said authentication in the end of a local from a terminal
The terminal characterized by providing.
[Claim 27]
The terminal authority authentication certificate lapse list table holding a terminal authority authentication certificate lapse list is provided further,
Said verification means makes a judgment with authentication failure, when said 2nd terminal authority authentication certificate is invalidated in said terminal authority authentication certificate lapse list held at said terminal authority authentication certificate lapse list table.
The terminal according to claim 26 characterized by things.
[Claim 28]
The procedure of receiving a signal including beacon information,
The procedure it is proposed to a said transmitting former terminal that carries out a terminal authority authentication certificate issue request if said signal does not show the purport in which the transmitting agency terminal of said signal has a terminal authority authentication certificate
The terminal authority authentication certificate issue proposal approach characterized by providing.
[Claim 29]
The procedure which acquires the terminal identification information on the terminal of these these others from said signal from a terminal besides the above is provided further,
Said proposal is performed based on said terminal identification information.
The terminal authority authentication certificate issue proposal approach according to claim 28 characterized by things.
[Claim 30]
The procedure of receiving a signal including beacon information,
The procedure which publishes the terminal authority authentication certificate which makes the concerned transmitting former terminal an owner if said signal does not show the purport in which the transmitting agency terminal of said signal has a terminal authority authentication certificate, and is proposed to the concerned transmitting former terminal
The terminal authority authentication certificate issue proposal approach characterized by providing.

[Claim 31]
The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
The procedure of receiving the proposal of the terminal authority authentication certificate issue request to said signal,
The procedure to which the information about the transmitting agency terminal of said proposal is displayed, and a check is urged,
The procedure which notifies refusal of a terminal authority authentication certificate issue proposal to a said transmitting former terminal when issue of a terminal authority authentication certificate is requested to a said transmitting former terminal when said check is made, and said check is refused
The terminal authority authentication certificate issue request approach to provide.
[Claim 32]
The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
The procedure of receiving the proposal of the terminal authority authentication certificate issue request to said signal,
The procedure to which the information about the transmitting agency terminal of said proposal is displayed, and a check is urged,
The procedure of requesting issue of a terminal authority authentication certificate to a said transmitting former terminal when the terminal authority authentication certificate concerned is received when said proposal contains the terminal authority authentication certificate [finishing / issue], if said check is made, and said proposal does not contain the terminal authority authentication certificate [finishing / issue]
The terminal authority authentication certificate issue request approach to provide.
[Claim 33]
The procedure of receiving a signal including beacon information,
if said signal is received from other terminals, terminal authority authentication certificate issue will be carried out -- as -- being concerned -- others -- the procedure requested to a terminal
The terminal authority authentication certificate issue request approach characterized by providing.
[Claim 34]
The procedure which acquires the terminal identification information on the terminal of these these others from said signal from a terminal besides the above is provided further,
Said request is performed based on said terminal identification information.
The terminal authority authentication certificate issue request approach according to claim 33 characterized by things.
[Claim 35]
The procedure of receiving a signal including beacon information,

The procedure it is proposed to a said transmitting former terminal that carries out a terminal authority authentication certificate issue request if said signal does not show the purport in which the transmitting agency terminal of said signal has a terminal authority authentication certificate
The program characterized by performing a terminal.
[Claim 36]
The procedure of receiving a signal including beacon information,
The procedure which publishes the terminal authority authentication certificate which makes the concerned transmitting former terminal an owner if said signal does not show the purport in which the transmitting agency terminal of said signal has a terminal authority authentication certificate, and is proposed to the concerned transmitting former terminal
The program characterized by performing a terminal.
[Claim 37]
The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
The procedure of receiving the proposal of the terminal authority authentication certificate issue request to said signal,
The procedure to which the information about the transmitting agency terminal of said proposal is displayed, and a check is urged,
The procedure which notifies refusal of a terminal authority authentication certificate issue proposal to a said transmitting former terminal when issue of a terminal authority authentication certificate is requested to a said transmitting former terminal when said check is made, and said check is refused
The program characterized by performing a terminal.
[Claim 38]
The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate,
The procedure of receiving the proposal of the terminal authority authentication certificate issue request to said signal,
The procedure to which the information about the transmitting agency terminal of said proposal is displayed, and a check is urged,
The procedure of requesting issue of a terminal authority authentication certificate to a said transmitting former terminal when the terminal authority authentication certificate concerned is received when said proposal contains the terminal authority authentication certificate [finishing / issue], if said check is made, and said proposal does not contain the terminal authority authentication certificate [finishing / issue]
The program characterized by performing a terminal.
[Claim 39]
The procedure of receiving a signal including beacon information,
if said signal is received from other terminals, terminal authority authentication

certificate issue will be carried out -- as -- being concerned -- others -- the procedure requested to a terminal
The program characterized by performing a terminal.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[Field of the Invention]
[0001]
This invention relates to the program which makes a computer (terminal) perform the terminal in the wireless ad hoc communication system which makes the access permission to a network attest especially using a terminal authority authentication certificate, and the system concerned, the art in these, and the approach concerned about wireless ad hoc communication system.
[Background of the Invention]
[0002]
The miniaturization of electronic equipment and high performance-ization progress, a terminal is connected to a network from it having become possible to carry simply and to use on the needed spot, and the environment which makes a communication link possible is searched for. Development of the network temporarily built as one if needed, i.e., a wireless ad hoc network technique, is furthered. In this wireless ad hoc network, without preparing a specific access point, each terminals (for example, a computer, a Personal Digital Assistant (PDA:Personal Digital Assistance), a cellular phone, etc.) carry out autonomous distribution, and are connected mutually.
[0003]
In order to prevent the device which generally does not have the authority connected to a certain network resource accessing, authority administration using a terminal authority authentication certificate is performed. As an example of this terminal authority authentication certificate, an attribute certificate is newly defined in March, 2000 by X.509 version 3, and the profile (definition of the contents of the data field contained in an attribute certificate) is summarized as specification (Standard Track RFC (Request For Comments)) of a standardization process from April, 2002. By using an attribute certificate as an access-permission certificate to a network resource, the authority linked to a network resource can be checked and connection can be permitted only to the terminal which holds connection rating. In addition, on these specifications, although an attribute certificate is explained as an example of a terminal authority authentication certificate, terminal authority is described with XML

language etc., and even if it seems that the engine which has authority was created by ****** which gives a signature to it, it may function as a terminal authority authentication certificate in this invention, for example.

[0004]

In the conventional communication system, the centralized control of the data used for authentication is carried out in the specific equipment on a network. For example, if one public key management equipment is shared with two or more radio switching systems and a migration terminal moves to the service area of a certain radio switching system, the technique of requiring the public key of the migration terminal of public key management equipment is proposed (for example, patent reference 1 reference.).

[Patent reference 1] JP,10-112883,A (drawing 1)

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0005]

Although the centralized control of the data used for authentication is carried out in the conventional communication system, in wireless ad hoc communication system, a terminal always moves, the terminals which therefore constitute a network each time differ, and the equipment which performs such a centralized control does not always exist. Moreover, on the property of a wireless medium, since the channel to the equipment which performs such a centralized control is not always secured, it is not suitable for a centralized control.

[0006]

Then, the purpose of this invention is in wireless ad hoc communication system to carry out autonomous distribution and perform issue of a terminal authority authentication certificate. All the wireless terminals of especially this invention that constitute a network are useful in the wireless network which transmits management information (for example, beacon etc.).

[Means for Solving the Problem]

[0007]

The 2nd terminal it is proposed to the 1st terminal of the above that the 1st terminal which transmits a signal including the beacon information which the wireless ad hoc communication system of this invention according to claim 1 is wireless ad hoc communication system constituted with two or more terminals, and shows the purport which does not have a terminal authority authentication certificate, and the above-mentioned signal are answered in order to solve the above-mentioned technical problem, and carries out a terminal authority authentication certificate issue request is provided. Operation of developing issue processing of a terminal authority authentication certificate between the 2nd terminal by making the signal from the 1st terminal into a trigger by this is brought about.

[0008]

moreover, the terminal of this invention according to claim 2 will carry out a terminal authority authentication certificate issue request, if the signal with which the receiving means and this receiving means for receiving a signal including beacon information include predetermined beacon information from other terminals is received -- as -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal is provided. Operation of developing issue processing of a terminal authority authentication certificate by making a signal including beacon information into a trigger by this is brought about.
[0009]
Moreover, the terminal of this invention according to claim 3 possesses further a means to acquire the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above which the above-mentioned receiving means received in a terminal according to claim 2, and the above-mentioned terminal authority authentication certificate issue proposal means performs the above-mentioned proposal based on the above-mentioned terminal identification information. The operation of making it propose, after this checks the terminal which should propose a terminal authority authentication certificate issue request is brought about.
[0010]
Moreover, in a terminal according to claim 2, in case the above-mentioned terminal authority authentication certificate issue proposal means proposes the above-mentioned terminal authority authentication certificate issue request to a terminal besides the above, the terminal of this invention according to claim 4 combines the public key certificate of the above-mentioned terminal, and is shown. The operation of making the transmit terminal of a signal including beacon information by this check this human nature of the terminal which proposed the terminal authority authentication certificate issue request is brought about.
[0011]
moreover -- if the terminal of this invention according to claim 5 receives the signal with which a receiving means to receive a signal including beacon information, and this receiving means include predetermined beacon information from other terminals -- being concerned -- others -- the terminal authority authentication certificate which makes a terminal an owner -- publishing -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal is provided. This brings about the operation of making a terminal authority authentication certificate publish in advance of a terminal authority authentication certificate issue request by making a signal including beacon information into a trigger.
[0012]
Moreover, the terminal of this invention according to claim 6 possesses further a means to acquire the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above

which the above-mentioned receiving means received in a terminal according to claim 5, and, as for the above-mentioned terminal authority authentication certificate issue proposal means, the above-mentioned proposal is performed based on the above-mentioned terminal identification information. The operation of making a terminal authority authentication certificate receive, after this checks the terminal which should propose a terminal authority authentication certificate issue request is brought about.

[0013]

Moreover, in a terminal according to claim 5, in case the above-mentioned terminal authority authentication certificate issue request is proposed to a terminal besides the above, the above-mentioned terminal authority authentication certificate issue proposal means combines the public key certificate of the above-mentioned terminal, and presents the terminal of this invention according to claim 7. The operation of making the transmit terminal of a signal including beacon information by this check this human nature of the terminal which proposed terminal authority authentication certificate issue is brought about.

[0014]

moreover, the case where the signal with which a receiving means and this receiving means for the terminal of this invention according to claim 8 to receive a signal including beacon information include beacon information from other terminals is received -- setting -- being concerned -- others -- if the above-mentioned signal does not show the purport in which a terminal has a terminal-authority authentication certificate, a terminal-authority authentication certificate issue request carries out -- as -- being concerned -- others -- a terminal-authority authentication certificate issue proposal means propose to a terminal provides. When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, operation of developing issue processing of a terminal authority authentication certificate by making the signal concerned into a trigger is brought about.

[0015]

Moreover, the terminal of this invention according to claim 9 possesses further a means to acquire the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above which the above-mentioned receiving means received in a terminal according to claim 8, and, as for the above-mentioned terminal authority authentication certificate issue proposal means, the above-mentioned proposal is performed based on the above-mentioned terminal identification information. The operation of making it propose, after this checks the terminal which should propose a terminal authority authentication certificate issue request is brought about.

[0016]

Moreover, in a terminal according to claim 8, in case the above-mentioned terminal

authority authentication certificate issue request is proposed to a terminal besides the above, the above-mentioned terminal authority authentication certificate issue proposal means combines the public key certificate of the above-mentioned terminal, and presents the terminal of this invention according to claim 10. The operation of making the transmit terminal of a signal including beacon information by this check this human nature of the terminal which proposed the terminal authority authentication certificate issue request is brought about.

[0017]

Moreover, the terminal of this invention according to claim 11 is set to a terminal according to claim 10. The terminal authority authentication certificate issue request receiving means for receiving a terminal authority authentication certificate issue request, this terminal authority authentication certificate issue request receiving means receives a terminal authority authentication certificate issue request from a terminal besides the above -- being concerned -- others -- with the check means to which the information about a terminal is displayed and a check is urged When the above-mentioned check is made, a terminal authority authentication certificate is published to a terminal besides the above, and when the above-mentioned check is refused, a terminal authority authentication certificate issue means to notify refusal of a terminal authority authentication certificate issue request to a terminal besides the above is provided further. The operation of making a terminal authority authentication certificate by this publish, after checking a terminal authority authentication certificate issue request terminal is brought about.

[0018]

Moreover, the terminal of this invention according to claim 12 is set to a terminal according to claim 11. The terminal authority authentication certificate issue terminal list table holding the public key certificate of a terminal authority authentication certificate issue terminal is provided further. The above-mentioned terminal authority authentication certificate issue means transmits the public key certificate of the above-mentioned terminal authority authentication certificate issue terminal held at the above-mentioned terminal authority authentication certificate issue terminal list table on the occasion of issue of the above-mentioned terminal authority authentication certificate to a terminal besides the above. This brings about operation of making easy verification of the terminal authority authentication certificate in other terminals.

[0019]

Moreover, in a terminal according to claim 11, the terminal authority authentication certificate lapse list table holding the lapse list of terminal authority authentication certificates is provided further, and the terminal of this invention according to claim 13 transmits the above-mentioned terminal authority authentication certificate lapse list with which the above-mentioned terminal authority authentication certificate issue means was held at the above-mentioned terminal authority authentication

certificate lapse list table on the occasion of issue of the above-mentioned terminal authority authentication certificate to a terminal besides the above. Thereby, in case a terminal authority authentication certificate is verified in other terminals, the operation of making the invalidated terminal authority authentication certificate eliminate is brought about.

[0020]

Moreover, a receiving means for the terminal of this invention according to claim 14 to receive a signal including beacon information, [when the signal with which this receiving means includes beacon information from other terminals is received] being concerned -- others -- if the above-mentioned signal does not show the purport in which a terminal has a terminal authority authentication certificate -- being concerned -- others -- the terminal authority authentication certificate which makes a terminal an owner -- publishing -- being concerned -- others -- a terminal authority authentication certificate issue proposal means to propose to a terminal is provided. When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, the operation of making a terminal authority authentication certificate publish in advance of a terminal authority authentication certificate issue request is brought about by making the signal concerned into a trigger.

[0021]

Moreover, the terminal of this invention according to claim 15 possesses further a means to acquire the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above which the above-mentioned receiving means received in a terminal according to claim 14, and the above-mentioned terminal authority authentication certificate issue proposal means performs the above-mentioned proposal based on the above-mentioned terminal identification information. The operation of making a terminal authority authentication certificate receive, after this checks the terminal which should propose a terminal authority authentication certificate issue request is brought about.

[0022]

Moreover, in a terminal according to claim 14, in case the above-mentioned terminal authority authentication certificate issue request is proposed to a terminal besides the above, the above-mentioned terminal authority authentication certificate issue proposal means combines the public key certificate of the above-mentioned terminal, and presents the terminal of this invention according to claim 16. The operation of making the transmit terminal of a signal including beacon information by this check this human nature of the terminal which proposed terminal authority authentication certificate issue is brought about.

[0023]

Moreover, a transmitting means to transmit that of the signal with which the terminal

of this invention according to claim 17 includes the beacon information which shows the purport which does not have a terminal authority authentication certificate, A terminal authority authentication certificate issue proposal receiving means to receive the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, this terminal authority authentication certificate issue proposal receiving means receives the above-mentioned proposal from other terminals -- being concerned -- others -- with the check means to which the information about a terminal is displayed and a check is urged When the above-mentioned check is made, issue of a terminal authority authentication certificate is requested to a terminal besides the above, and when the above-mentioned check is refused, a terminal authority authentication certificate issue request means to notify refusal of a terminal authority authentication certificate issue proposal to a terminal besides the above is provided. The operation of making issue of a terminal authority authentication certificate by this request, after checking a terminal authority authentication certificate issue terminal is brought about.

[0024]

Moreover, in a terminal according to claim 17, in case the above-mentioned terminal authority authentication certificate issue is requested to a terminal besides the above, the above-mentioned terminal authority authentication certificate issue request means combines the public key certificate of the above-mentioned terminal, and presents the terminal of this invention according to claim 18. The operation of making a terminal authority authentication certificate issue terminal by this check this human nature of the terminal which carried out the terminal authority authentication certificate issue request is brought about.

[0025]

Moreover, a transmitting means to transmit the signal with which the terminal of this invention according to claim 19 includes the beacon information which shows the purport which does not have a terminal authority authentication certificate, A terminal authority authentication certificate issue proposal receiving means to receive the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, this terminal authority authentication certificate issue proposal receiving means receives the above-mentioned proposal from other terminals -- being concerned -- others -- with the check means to which the information about a terminal is displayed and a check is urged If the above-mentioned check is made, when the above-mentioned proposal contains the terminal authority authentication certificate [finishing / issue], the terminal authority authentication certificate concerned is received. When the above-mentioned proposal does not contain the terminal authority authentication certificate [finishing / issue], a terminal authority authentication certificate issue request means to request issue of a terminal authority authentication certificate to a terminal besides the above is provided. Thereby, when the proposal of a terminal authority authentication certificate issue

request is received, the proposal judges whether the terminal authority authentication certificate [finishing / issue] is included, and brings about operation of operating whether a terminal authority authentication certificate being received or issue of a terminal authority authentication certificate being requested.

[0026]

Moreover, in a terminal according to claim 19, in case the above-mentioned terminal authority authentication certificate issue is requested to a terminal besides the above, the above-mentioned terminal authority authentication certificate issue request means combines the public key certificate of the above-mentioned terminal, and presents the terminal of this invention according to claim 20. The operation of making a terminal authority authentication certificate issue terminal by this check this human nature of the terminal which carried out the terminal authority authentication certificate issue request is brought about.

[0027]

Moreover, the terminal of this invention according to claim 21 possesses a terminal authority authentication certificate issue request means to request to a terminal besides the above to carry out terminal authority authentication certificate issue, if the signal with which a receiving means to receive a signal including beacon information, and this receiving means include predetermined beacon information from other terminals is received. The operation of this answering reception of a signal including beacon information, and making terminal authority authentication certificate issue request is brought about.

[0028]

Moreover, the terminal of this invention according to claim 22 possesses further a means to acquire the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above which the above-mentioned receiving means received in a terminal according to claim 21, and, as for a terminal authority authentication certificate issue request means, the above-mentioned proposal is performed based on the above-mentioned terminal identification information. The operation of making it request, after this checks the terminal which should request issue of a terminal authority authentication certificate is brought about.

[0029]

Moreover, the terminal authority authentication certificate table holding the 1st terminal authority authentication certificate which the terminal of this invention according to claim 23 shows the access permission in the end of a local, The receiving means for receiving a signal including beacon information, [when the signal with which this receiving means includes beacon information from other terminals is received] The terminal authority authentication certificate of the above 1st held at the above-mentioned terminal authority authentication certificate table when the above-mentioned signal showed the purport which a terminal has is shown. being

concerned -- others -- the 2nd terminal authority authentication certificate in which the access permission of a terminal is shown -- being concerned -- others -- An authentication demand means to require the authentication in the above-mentioned end of a local from a terminal besides the above is provided. Operation of developing the mutual recognition processing based on a terminal authority authentication certificate is brought about by making into a trigger the signal which includes by this the beacon information from other terminals that it has a terminal authority authentication certificate.

[0030]

Moreover, the terminal of this invention according to claim 24 is set to a terminal according to claim 23. The terminal authority authentication certificate issue terminal list table holding the public key certificate of a terminal authority authentication certificate issue terminal, An authentication demand receiving means to receive the 2nd authentication demand which answers the authentication demand by the above-mentioned authentication demand means, and a terminal besides the above requires, A verification means to verify the terminal authority authentication certificate of the above 2nd included in the authentication demand of the above 2nd which this authentication demand receiving means received with the public key contained in the public key certificate held at the above-mentioned terminal authority authentication certificate issue terminal list table is provided further. The operation of making the accepting station of the signal concerned verify the terminal authority authentication certificate which this shows the access permission of the transmit terminal of a signal including beacon information is brought about.

[0031]

Moreover, in a terminal according to claim 24, the terminal authority authentication certificate lapse list table holding a terminal authority authentication certificate lapse list is provided further, and the terminal of this invention according to claim 25 carries out decision with authentication failure, when invalidated in the terminal authority authentication certificate of the above 2nd in the above-mentioned terminal authority authentication certificate lapse list with which the above-mentioned verification means is held at the above-mentioned terminal authority authentication certificate lapse list table. Thereby, in case a terminal authority authentication certificate is verified in the terminal concerned, the operation of making the invalidated terminal authority authentication certificate eliminate is brought about.

[0032]

Moreover, the terminal authority authentication certificate issue terminal list table with which the terminal of this invention according to claim 26 holds the public key certificate of a terminal authority authentication certificate issue terminal, A transmitting means to transmit a signal including the beacon information which shows the purport which has the 2nd terminal authority authentication certificate to other terminals which have the 1st terminal authority authentication certificate, The

terminal authority authentication certificate table holding the terminal authority authentication certificate of the above 2nd in which the access permission in the end of a local is shown, An authentication demand receiving means to receive the 1st authentication demand from other terminals to the above-mentioned signal, A verification means to verify the terminal authority authentication certificate of the above 1st included in the authentication demand of the above 1st which this authentication demand receiving means received with the public key contained in the public key certificate held at the above-mentioned terminal authority authentication certificate issue terminal list table, If authentication succeeds in this verification means, an authentication demand means to perform the 2nd authentication demand which presents the terminal authority authentication certificate of the above 2nd held to the terminal besides the above at the above-mentioned terminal authority authentication certificate table, and requires the authentication in the above-mentioned end of a local from a terminal besides the above is provided. Operation of developing the mutual recognition processing based on a terminal authority authentication certificate is brought about by making into a trigger a signal including the beacon information which shows by this the purport which has a terminal authority authentication certificate.

[0033]

Moreover, in a terminal according to claim 26, the terminal authority authentication certificate lapse list table holding a terminal authority authentication certificate lapse list is provided further, and the terminal of this invention according to claim 27 carries out decision with authentication failure, when invalidated in the terminal authority authentication certificate of the above 2nd in the above-mentioned terminal authority authentication certificate lapse list with which the above-mentioned verification means is held at the above-mentioned terminal authority authentication certificate lapse list table. Thereby, in case a terminal authority authentication certificate is verified in the terminal concerned, the operation of making the invalidated terminal authority authentication certificate eliminate is brought about.

[0034]

Moreover, the terminal authority authentication certificate issue proposal approach of this invention according to claim 28 possesses the procedure of receiving a signal including beacon information, and the procedure it is proposed to the above-mentioned transmitting agency terminal that carry out a terminal authority authentication certificate issue request if the above-mentioned signal does not show the purport in which the transmitting agency terminal of the above-mentioned signal has a terminal authority authentication certificate. When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, operation of developing issue processing of a terminal authority authentication certificate by making the signal concerned into a trigger is brought about.

[0035]
Moreover, in the terminal authority authentication certificate issue proposal approach according to claim 28, the terminal authority authentication certificate issue proposal approach of this invention according to claim 29 possesses further the procedure which acquires the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above, and performs the above-mentioned proposal based on the above-mentioned terminal identification information. The operation of making it propose, after this checks the terminal which should propose a terminal authority authentication certificate issue request is brought about.
[0036]
Moreover, the terminal authority authentication certificate issue proposal approach of this invention according to claim 30 possesses the procedure which publishes the terminal authority authentication certificate which makes the concerned transmitting former terminal an owner, and is proposed to the concerned transmitting former terminal, if the above-mentioned signal does not show the procedure of receiving a signal including beacon information, and the purport in which the transmitting agency terminal of the above-mentioned signal has a terminal authority authentication certificate. When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, the operation of making a terminal authority authentication certificate publish in advance of a terminal authority authentication certificate issue request is brought about by making the signal concerned into a trigger.
[0037]
Moreover, the terminal authority authentication certificate issue request approach of this invention according to claim 31 The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate, The procedure of receiving the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, The procedure to which the information about the transmitting agency terminal of the above-mentioned proposal is displayed, and a check is urged, and when the above-mentioned check is made, issue of a terminal authority authentication certificate is requested to the above-mentioned transmitting agency terminal. When the above-mentioned check is refused, the procedure which notifies refusal of a terminal authority authentication certificate issue proposal to the above-mentioned transmitting agency terminal is provided. The operation of making issue of a terminal authority authentication certificate by this request, after checking a terminal authority authentication certificate issue terminal is brought about.
[0038]
Moreover, the terminal authority authentication certificate issue request approach of this invention according to claim 32 The procedure of transmitting a signal including

the beacon information which shows the purport which does not have a terminal authority authentication certificate, The procedure of receiving the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, If the procedure to which the information about the transmitting agency terminal of the above-mentioned proposal is displayed, and a check is urged, and the above-mentioned check are made When the above-mentioned proposal contains the terminal authority authentication certificate [finishing / issue], the terminal authority authentication certificate concerned is received, and when the above-mentioned proposal does not contain the terminal authority authentication certificate [finishing / issue], the procedure of requesting issue of a terminal authority authentication certificate to the above-mentioned transmitting agency terminal is provided. Thereby, when the proposal of a terminal authority authentication certificate issue request is received, the proposal judges whether the terminal authority authentication certificate [finishing / issue] is included, and brings about operation of operating whether a terminal authority authentication certificate being received or issue of a terminal authority authentication certificate being requested.

[0039]

moreover, the terminal authority authentication certificate issue request approach of this invention according to claim 33 will carry out terminal authority authentication certificate issue to the procedure of receiving a signal including beacon information, if the above-mentioned signal is received from other terminals -- as -- being concerned -- others -- the procedure requested to a terminal is provided. The operation of this answering reception of a signal including beacon information, and making terminal authority authentication certificate issue request is brought about.

[0040]

Moreover, in the terminal authority authentication certificate issue request approach of this invention according to claim 33, the terminal authority authentication certificate issue request approach of this invention according to claim 34 possesses further the procedure which acquires the terminal identification information on the terminal of these these others from the above-mentioned signal from a terminal besides the above, and performs the above-mentioned request based on the above-mentioned terminal identification information. The operation of making it request, after this checks the terminal which should request issue of a terminal authority authentication certificate is brought about.

[0041]

Moreover, the program of this invention according to claim 35 makes a terminal perform the procedure of receiving a signal including beacon information, and the procedure it is proposed to the above-mentioned transmitting agency terminal that carry out a terminal authority authentication certificate issue request if the above-mentioned signal does not show the purport in which the transmitting agency terminal of the above-mentioned beacon has a terminal authority authentication certificate.

When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, operation of developing issue processing of a terminal authority authentication certificate by making the signal concerned into a trigger is brought about.

[0042]

Moreover, the program of this invention according to claim 36 makes a terminal perform the procedure which publishes the terminal authority authentication certificate which makes the concerned transmitting former terminal an owner, and is proposed to the concerned transmitting former terminal, if the above-mentioned signal does not show the procedure of receiving a signal including beacon information, and the purport in which the transmitting agency terminal of the above-mentioned signal has a terminal authority authentication certificate. When the transmit terminal of a signal including beacon information does not have the terminal authority authentication certificate by this, the operation of making a terminal authority authentication certificate publish in advance of a terminal authority authentication certificate issue request is brought about by making the signal concerned into a trigger.

[0043]

Moreover, the program of this invention according to claim 37 The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate, The procedure of receiving the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, The procedure to which the information about the transmitting agency terminal of the above-mentioned proposal is displayed, and a check is urged, and when the above-mentioned check is made, issue of a terminal authority authentication certificate is requested to the above-mentioned transmitting agency terminal. When the above-mentioned check is refused, a terminal is made to perform the procedure which notifies refusal of a terminal authority authentication certificate issue proposal to the above-mentioned transmitting agency terminal. The operation of making issue of a terminal authority authentication certificate by this request, after checking a terminal authority authentication certificate issue terminal is brought about.

[0044]

Moreover, the program of this invention according to claim 38 The procedure of transmitting a signal including the beacon information which shows the purport which does not have a terminal authority authentication certificate, The procedure of receiving the proposal of the terminal authority authentication certificate issue request to the above-mentioned signal, If the procedure to which the information about the transmitting agency terminal of the above-mentioned proposal is displayed, and a check is urged, and the above-mentioned check are made When the above-mentioned proposal contains the terminal authority authentication certificate

[finishing / issue], the terminal authority authentication certificate concerned is received. When the above-mentioned proposal does not contain the terminal authority authentication certificate [finishing / issue], a terminal is made to perform the procedure of requesting issue of a terminal authority authentication certificate to the above-mentioned transmitting agency terminal. Thereby, when the proposal of a terminal authority authentication certificate issue request is received, the proposal judges whether the terminal authority authentication certificate [finishing / issue] is included, and brings about operation of operating whether a terminal authority authentication certificate being received or issue of a terminal authority authentication certificate being requested.

[0045]

moreover, the program of this invention according to claim 39 will carry out terminal authority authentication certificate issue to the procedure of receiving a signal including beacon information, if the above-mentioned signal is received from other terminals -- as -- being concerned -- others -- a terminal is made to perform the procedure requested to a terminal The operation of this answering reception of a signal including beacon information, and making terminal authority authentication certificate issue request is brought about.

[Effect of the Invention]

[0046]

According to this invention, in wireless ad hoc communication system, the outstanding effectiveness of if autonomous distribution can be carried out and issue of a terminal authority authentication certificate can be performed can be done so.

[Best Mode of Carrying Out the Invention]

[0047]

Next, the gestalt of operation of this invention is explained to a detail with reference to a drawing.

[0048]

Drawing 1 is drawing showing the example of a configuration of the wireless terminal 300 used in the wireless ad hoc communication system in the gestalt of operation of this invention. The wireless terminal 300 is equipped with the communications processing section 320, a control section 330, a display 340, a control unit 350, a loudspeaker 360, a microphone 370, and memory 600, and has the composition that a bus 380 connects between these. Moreover, the antenna 310 is connected to the communications processing section 320. The communications processing section 320 constitutes the frame of a network interface layer (data link layer) from a signal received through the antenna 310. Moreover, the communications processing section 320 transmits the frame of a network interface layer through an antenna 310.

[0049]

A control section 330 controls the wireless terminal 300 whole. For example, predetermined processing is performed with reference to the frame constituted by

the communications processing section 320. A display 340 displays predetermined information and a liquid crystal display etc. may be used. A control unit 350 is for performing operator guidance from the exterior to the wireless terminal 300, for example, a keyboard, a button switch, etc. may be used. A loudspeaker 360 outputs voice, and it is used in order to call attention or to perform the exchange of other terminals and speech information to the user of the wireless terminal 300. A microphone 370 is used in order to perform voice input from the exterior to the wireless terminal 300, to perform the exchange of other terminals and speech information or to perform operator guidance.

[0050]

The attribute certificate issue terminal list table 610 holding the information concerning [memory 600] the issue terminal of an attribute certificate, The attribute certificate table 620 holding the attribute certificate in which the access permission of wireless terminal 300 self is shown, The attribute certificate lapse list table 630 holding the information about the invalidated attribute certificate and the generation key table 650 which holds a public key, a private key, and a public key certificate as information about the generation key of wireless terminal 300 self are stored.

[0051]

Drawing 2 is the example of a configuration of the attribute certificate issue terminal list table 610 in the gestalt of operation of this invention. This attribute certificate issue terminal list table 610 holds the information about a terminal with the track record of having published the attribute certificate in the past, and holds the public key certificate 612 corresponding to each of the terminal identification child 611 of an attribute certificate issue terminal. The terminal identification child 611 can use the MAC (Media Access Control) address in Ethernet (trademark) etc. that what is necessary is just what identifies a terminal in a network at a meaning. The public key certificate 612 is a public key certificate of the terminal identified by the corresponding terminal identification child 611. A public key certificate proves this human nature of a certificate owner (subject), and contains a certificate owner's public key. This public key certificate is signed by the certificate publisher slack certificate authority (CA:Certificate Authority).

[0052]

Drawing 3 is drawing showing the format 710 of the public key certificate 612 held at the attribute certificate issue terminal list table 610. The format 710 of this public key certificate is roughly divided, and consists of a certificate 711 before a signature, a signature algorithm 718, and signature 719. The certificate 711 before a signature contains a serial number 712, a publisher 714, an expiration date 715, an owner 716, an owner 716, and the owner public key 717.

[0053]

A serial number 712 is a serial number of a public key certificate, and is ****(ed) by the certificate authority. A publisher 714 is the identifier of the publisher slack

certificate authority of a public key certificate. A public key certificate is identified by the meaning by this publisher 714 and serial number 712. An expiration date 715 is an expiration date of a public key certificate. An owner 716 is the identifier of the owner of a public key certificate. The owner public key 717 is an owner's 716 public key.
[0054]
Signature 719 is a signature by the certificate authority to a public key certificate, and the signature algorithm 718 is a signature algorithm used for this signature 719. A signature algorithm is constituted by two, a message digest algorithm and a public-key-encryption algorithm. A message digest algorithm is one of the Hash Functions (epitome function), and is an algorithm for creating the message digest of the certificate 711 before a signature. Here, with a message digest, input data (front [signature] certificate 711) is compressed into a fixed-length bit string, and it is called a thumbmark, a fingerprint (fingerprints), etc. As a message digest algorithm, SHA-1 (Secure Hash Algorithm 1), MD2 (Message Digest #2), MD5 (Message Digest #5), etc. are known. A public-key-encryption algorithm is an algorithm for enciphering the message digest obtained by the message digest algorithm with the private key of a certificate authority. RSA based on a factorization-in-prime-numbers problem as this public-key-encryption algorithm, and dispersion -- a logarithm -- DSA based on a problem etc. is known. Thus, what enciphered the message digest of the certificate 711 before a signature with the private key of a certificate authority serves as signature 719.
[0055]
Therefore, a message digest is obtained by decoding the signature 719 of this public key certificate with the public key of a certificate authority. The user of a public key certificate can verify that the contents of the certificate 711 before a signature are not altered by creating the message digest of the certificate 711 before a signature in person, and comparing it with the message digest decoded with the public key of a certificate authority.
[0056]
Drawing 4 is drawing showing the format 720 of the attribute certificate held at the attribute certificate table 620. This attribute certificate is roughly divided and consists of attribute certification information 721, a signature algorithm 728, and signature 729. The attribute certification information 721 contains the owner public key certificate identifier 723, a publisher 724, a serial number 722, and an expiration date 725.
[0057]
The owner public key certificate identifier 723 is for identifying the public key certificate of the owner of an attribute certificate. Specifically, it identifies by the publisher 714 and serial number 712 of the public key certificate 710 (drawing 3). In addition, you may make it this public key certificate identifier 723 use an owner's MAC Address etc. that what is necessary is just what has the function to identify an

owner. A publisher 724 is the name of the publisher slack attribute certificate authority (AA:Attribute certificate Authority) of an attribute certificate, for example, can use a publisher's MAC Address etc. A serial number 722 is a serial number of an attribute certificate, and is ****(ed) by the publisher slack attribute certificate authority of an attribute certificate. An attribute certificate is identified by this serial number 722 and publisher 724 at a meaning. An expiration date 725 is an expiration date of an attribute certificate.

[0058]

Signature 729 is a signature by the attribute certificate authority to an attribute certificate, and the signature algorithm 728 is a signature algorithm used for this signature 729. About the contents of the signature algorithm, it is the same as that of the signature algorithm 718 of the above-mentioned public key certificate, and what enciphered the message digest of the attribute certification information 721 with the private key of an attribute certificate authority serves as signature 729.

[0059]

Therefore, a message digest is obtained by decoding the signature 729 of this attribute certificate with the public key of an attribute certificate authority. The user of an attribute certificate can verify that the contents of the attribute certification information 721 are not altered by creating the message digest of the attribute certification information 721 in person, and comparing it with the message digest decoded with the public key of an attribute certificate authority.

[0060]

Drawing 5 is the example of a configuration of the attribute certificate lapse list table 630 in the gestalt of operation of this invention. This attribute certificate lapse list table 630 holds the information about the invalidated attribute certificate, and holds the pair of the attribute certificate identifier 631 and the invalidated lapse time of day 632 of the invalidated attribute certificate. When the case where a terminal is lost, and a theft are encountered, in order to invalidate an attribute certificate compulsorily, an attribute certificate lapse list (ARL:Attribute certificate Revocation List) is published. The pair of the attribute certificate identifier 631 and the lapse time of day 632 is extracted from each lapse list entry of an attribute certificate lapse list, and is held. The attribute certificate identifier 631 is for identifying the invalidated attribute certificate, and, specifically, is identified by the publisher 724 and serial number 722 of the attribute certificate 720 (drawing 4).

[0061]

Drawing 6 is drawing showing a format of the attribute certificate lapse list 730. This attribute certificate lapse list is roughly divided, and consists of a lapse list 731 before a signature, a signature algorithm 738, and signature 739. The lapse list 731 before a signature contains the publisher 734 of the lapse list before a signature, and zero or more lapse list entries 735. The lapse list entry 735 is the pair of the attribute certificate identifier 736 and the invalidated lapse time of day 737 of the invalidated

attribute certificate. The pair of the attribute certificate identifier 736 and the lapse time of day 737 in this lapse list entry 735 corresponds to the pair of the attribute certificate identifier 631 and the lapse time of day 632 in the attribute certificate lapse list table 630 (drawing 5).

[0062]

Signature 739 is a signature by the publisher to an attribute certificate lapse list, and the signature algorithm 738 is a signature algorithm used for this signature 739. About the contents of the signature algorithm, it is the same as that of the signature algorithm 718 of the above-mentioned public key certificate, and what enciphered the message digest of the lapse list 731 before a signature with a publisher's private key serves as signature 739.

[0063]

Therefore, a message digest is obtained by decoding the signature 739 of this attribute certificate lapse list with a publisher's public key. The user of an attribute certificate lapse list can verify that the contents of the lapse list 731 before a signature are not altered by creating the message digest of the lapse list 731 before a signature in person, and comparing it with the message digest decoded with a publisher's public key.

[0064]

In addition, in wireless ad hoc communication system, since it is difficult to assume existence of the fixed server which carries out the centralized control of the attribute certificate lapse list, all the terminals that constitute a network shall publish an attribute certificate lapse list. The terminal which published the attribute certificate lapse list can verify the effectiveness of an attribute certificate also in other terminals by carrying out broadcasting distribution of the attribute certificate lapse list to other terminals. Moreover, when it re-connects with a network, each terminal exchanges an attribute certificate lapse list mutually, and the newest condition is maintained by merging the attribute certificate lapse list table 630. In addition, it is desirable to attach a public key certificate and an attribute certificate so that a publisher can be easily attested in the case of attribute certificate lapse list issue.

[0065]

Next, actuation of the wireless ad hoc communication system in the gestalt of operation of this invention is explained with reference to a drawing. With the gestalt of operation of this invention, in order for a terminal to connect with a network resource, it is supposed that the procedure (drawing 7 or drawing 15) of "initial registration" in which a terminal receives issue of an attribute certificate, and the procedure (drawing 18) of "mutual recognition" in which a terminal attests using an attribute certificate will be completed. Each processing in these drawing 7 , drawing 15 , and drawing 18 is realized by the control section 330 in the wireless terminal 300.

[0066]

Drawing 7 is drawing showing the 1st example of the procedure of the initial

registration in the gestalt of operation of this invention. Here, Terminal A (100) is an attribute certificate issue terminal which has already entered into the network, and Terminal B (200) is a terminal which is going to enter into the network newly.

[0067]

Each terminal in wireless ad hoc communication system transmits a beacon periodically, in order to tell other terminals about existence of self. In the gestalt of operation of this invention, a beacon includes not only a signal only including the beacon information as an identification signal but the signal with which a certain data information was added to beacon information. In the example of this drawing 7 , Terminal A received the beacon 2011 which Terminal B transmitted (201) (101), and Terminal B has received the beacon 1022 which Terminal A transmitted (102) (202). Thereby, Terminal A and Terminal B grasp a mutual terminal identification child with the frame structure of the following beacons.

[0068]

The frame structure of these beacons 2011 and 1022 is as drawing 8 . The beacon frame 810 consists of a header unit 811 and the payload section 812. Moreover, a header unit 811 contains the starting point terminal identification child 813, the terminal point terminal identification child 814, the transmit-terminal identifier 815, received terminal identification 816, the frame classification 817, and the existence 818 of an attribute certificate. The starting point terminal identification child 813 is a terminal identification child of the terminal which sent this frame first. In addition, a terminal identification child can use the MAC Address in Ethernet (trademark) etc. that what is necessary is just what identifies a terminal in a network as mentioned above at a meaning. The terminal point terminal identification child 814 is a terminal identification child of the terminal of the final destination of this frame. With the beacon frame 810, a broadcast address (for example, all bits 1) is assigned to this terminal point terminal identification child 814.

[0069]

The transmit-terminal identifier 815 and received terminal identification 816 are used in case a frame is relayed. In wireless ad hoc communication system, it restricts that no the direct communication of the terminals in a network can be carried out, but a communication path must be established by multi-hop through other terminals to transmit a frame to the terminal which an electric wave does not reach. In this case, the transmit-terminal identifier 815 and received terminal identification 816 are used between the terminals which transmit and receive a frame.

[0070]

The frame classification 817 shows the classification of a frame and shows that it is a beacon frame here. The existence 818 of an attribute certificate shows whether the transmitting agency terminal of a beacon frame has the attribute certificate in which the authority to access a network resource is shown. By the initial registration sequence of drawing 7 , since Terminal B does not have the attribute certificate, the

purport "which it does not have" is shown in the existence 818 of this attribute certificate. In addition, with an example of this beacon frame, other information is not included in the data 819 of the payload section 812.
[0071]
Terminal A will check the existence 818 of the starting point terminal identification child 814 of the beacon frame 810, and an attribute certificate, if the beacon 2011 transmitted from Terminal B is received (101). If it judges that the terminal B which is a starting point terminal does not have the attribute certificate, the attribute certificate issue proposal message 1032 proposed that Terminal A carries out an attribute certificate issue request to Terminal B will be transmitted (103). In addition, although the existence of the attribute certificate shown in a beacon supposing transmitting an attribute certificate issue proposal message automatically here is verified, Terminal A creates an attribute certificate issue proposal message to Terminal B, and you may make it transmit it to the timing of arbitration, without checking the existence of this attribute certificate.
[0072]
The frame structure of this attribute certificate issue proposal message 1032 is as drawing 9 . The attribute certificate issue proposal frame 820 consists of a header unit 821 and the payload section 822. A header unit 821 includes the starting point terminal identification child 823, the terminal point terminal identification child 824, the transmit-terminal identifier 825, received terminal identification 826, and the frame classification 827. About the contents in these header units 821, it is the same as that of the beacon frame 810 explained by drawing 8 . Moreover, with this attribute certificate issue proposal frame 820, the public key certificate 8291 of the terminal A which is a transmitting agency is contained as data 829 of the payload section 822. The public key certificate 8291 of this terminal A is beforehand stored in the generation key table 650 of Terminal A. In addition, as data 829, a terminal identification child etc. may also be included besides the public key certificate 8291.
[0073]
Terminal B will check Terminal A from the contents, if the attribute certificate issue proposal message 1032 transmitted from Terminal A is received (203). For example, decision whether it is a right attribute certificate issue terminal is demanded from a user by displaying the owner 716 (drawing 3) of the public key in the starting point terminal identification child 823 (drawing 9) and the public key certificate 8291 of the attribute certificate issue proposal frame 820 on a display 340 (drawing 1). Thereby, the break in of a terminal with the malice by address forgery etc. or the terminal which is not meant can be prevented. It is the terminal which the terminal A of a transmitting agency trusts, and in meaning that I have Terminal A publish an attribute certificate, a user performs confirmation operation by the control unit 350 (drawing 1).
[0074]

If a proposal is accepted by the user validation (203), Terminal B will transmit the attribute certificate issue request message 2041 which requests attribute certificate issue to Terminal A (204). The frame structure of this attribute certificate issue request message 2041 is as drawing 9 , and is the same as that of the frame 820 of the attribute certificate issue proposal message 1032. The same is said of the point that the public key certificate 8391 of the terminal B which is a transmitting agency as data 839 of the payload section 832 is contained.

[0075]

In addition, when a proposal is refused by the user validation (203), you may make it Terminal B transmit the attribute certificate issue proposal refusal message which notifies refusal of an attribute certificate issue proposal to Terminal A. The frame structure of this attribute certificate issue proposal refusal message is as drawing 10 . The attribute certificate issue proposal refusal frame 840 consists of a header unit 841 and the payload section 842. A header unit 841 includes the starting point terminal identification child 843, the terminal point terminal identification child 844, the transmit-terminal identifier 845, received terminal identification 846, the frame classification 847, and the refusal reason classification 848. Although it is the same as that of the beacon frame 810 explained by drawing 8 about the contents in these header units 841, about the refusal reason classification 848, it is peculiar to this attribute certificate issue proposal refusal frame 840. It cancels in this refusal reason classification 848 according to a user, and the reason of not trusting it as an attribute certificate authority is coded and shown in it.

[0076]

Terminal A will check Terminal B from the contents, if the attribute certificate issue request message 2041 transmitted from Terminal B is received (104). For example, decision whether it is the terminal which he can trust is demanded from a user by displaying the owner 716 (drawing 3) of the public key in the starting point terminal identification child 833 (drawing 9) and the public key certificate 8391 of the attribute certificate issue request frame 830 on a display 340 (drawing 1). If it is the terminal which the terminal B of a transmitting agency trusts, a user will perform confirmation operation by the control unit 350 (drawing 1).

[0077]

If a check is made by the user, Terminal A will transmit the attribute certificate issue message 1052 to Terminal B, in order to publish an attribute certificate (105). The frame structure of this attribute certificate issue message 1052 is as drawing 11 . The attribute certificate issue frame 860 consists of a header unit 861 and the payload section 862. A header unit 861 includes the starting point terminal identification child 863, the terminal point terminal identification child 864, the transmit-terminal identifier 865, received terminal identification 866, and the frame classification 867. About the contents in these header units 861, it is the same as that of the attribute certificate issue proposal frame 820 explained by drawing 9 . Moreover, with this

attribute certificate issue frame 860, the attribute certificate 8691 signed with Terminal A as data 869 of the payload section 862 by making into an owner the terminal B which is a requesting agency is contained. The terminal B which received the attribute certificate issue message 1052 from Terminal A (205) extracts the attribute certificate 8691 from the attribute certificate issue frame 860, and stores it in the attribute certificate table 620.

[0078]

In addition, when a check (104) is refused by the user, you may make it Terminal A transmit the attribute certificate issue request refusal message which notifies refusal of an attribute certificate issue request to Terminal B. The frame structure of this attribute certificate issue request refusal message is as drawing 10 , and is the same as that of the attribute certificate issue proposal refusal frame 840.

[0079]

Drawing 12 is drawing showing the modification of the 1st example of the initial registration procedure in the gestalt of operation of this invention. In this modification, in case an attribute certificate issue proposal message is transmitted from an attribute certificate issue terminal, the number of messages exchanged between terminals is reduced by publishing an attribute certificate and attaching to that message. The point that Terminal A (100) is an attribute certificate issue terminal, and Terminal B (200) is a new-comer terminal here is the same as the 1st example of drawing 7 . When the point of transmitting each other's beacon also has the same end of both ends, Terminal A receives the beacon 2311 which Terminal B transmitted (231) (131) and Terminal B receives the beacon 1322 which Terminal A transmitted (132) (232), Terminal A and Terminal B grasp a mutual terminal identification child. It is as drawing 8 having explained the frame structure of these beacons as well as the 1st example.

[0080]

In the example of this drawing 12 , an attribute certificate is published to the terminal B (200) which is a new-comer terminal, without the terminal A (100) which is an attribute certificate issue terminal which received the beacon receiving an attribute certificate issue request message (2041 of drawing 7) unlike the 1st example of drawing 7 , and it includes and transmits to the data of the payload section of the attribute certificate issue proposal message 1332. The signature by Terminal A is made by this attribute certificate by making into an owner the terminal B which is an issue place. The frame structure 1820 of the attribute certificate issue proposal message 1332 in this case is as drawing 13 , and has the frame structure 820 of the attribute certificate issue proposal message of drawing 9 , and same composition except for the point which contains the attribute certificate 18292 to the end of an issue tip as data 1829 of the payload section 1822. This becomes possible to reduce the number of messages compared with the 1st example of drawing 7 . In addition, it may be made to judge whether an attribute certificate issue proposal message

contains the attribute certificate 18292 by the frame classification 827 or 1827 in Terminal B (200), and it prepares the field separately and you may make it judge it according to the contents of the field.

[0081]

In the example of drawing 12 , Terminal B (200) will check Terminal A (100) from the contents, if the attribute certificate issue proposal message 1332 transmitted from Terminal A (100) (133) is received (233). For example, decision whether it is a right attribute certificate issue terminal is demanded from a user by displaying the starting point terminal identification child 1823 of the attribute certificate issue proposal frame 1820. Thereby, the break in of a terminal with the malice by address forgery etc. or the terminal which is not meant can be prevented. In receiving the attribute certificate which is the terminal which the terminal A of a transmitting agency (100) trusts, and Terminal A (100) published, a user performs confirmation operation by the control unit 350 (drawing 1). The terminal B (200) which accepted the attribute certificate issue proposal message 1332 from Terminal A (100) extracts the attribute certificate 18292 from the payload section 1822 of the attribute certificate issue proposal frame 1820, and stores it in the attribute certificate table 620 (drawing 1).

[0082]

If a check (233) is made by the user, Terminal B (200) will transmit the attribute certificate issue proposal receipt message 2341 which receives the attribute certificate issue proposal message 1332 to Terminal A (100) (234). The frame structure 1830 of this attribute certificate issue proposal receipt message 2341 is as drawing 14 , and has a frame structure of the attribute certificate issue request message of drawing 9 , and same composition fundamentally.

[0083]

In addition, when a proposal is refused by the user validation (233), you may make it Terminal B (200) transmit the attribute certificate issue proposal refusal message which notifies refusal of an attribute certificate issue proposal to Terminal A. The frame structure 840 of this attribute certificate issue proposal refusal message is the same configuration as what was explained by drawing 10 .

[0084]

Drawing 15 is drawing showing the 2nd example of the procedure of the initial registration in the gestalt of operation of this invention. The point that Terminal A (100) is an attribute certificate issue terminal, and Terminal B (200) is a new-comer terminal is the same as the 1st example of drawing 7 . When the point of transmitting each other's beacon also has the same end of both ends, Terminal A receives the beacon 2211 which Terminal B transmitted (221) (121) and Terminal B receives the beacon 1222 which Terminal A transmitted (122) (222), Terminal A and Terminal B grasp a mutual terminal identification child. The frame structure of these beacons 2211 and 1222 is as drawing 8 similarly.

[0085]

In the 2nd example of this drawing 15 , the attribute certificate issue request message 2251 is transmitted to the terminal A which is an attribute certificate issue terminal, without the terminal B which is a new-comer terminal which received the beacon receiving an attribute certificate issue proposal message unlike the 1st example of drawing 7 (225). The frame structure 830 of this attribute certificate issue request message 2041 is as drawing 9 having explained. Under the present circumstances, when Terminal B does not have the public key certificate of the terminal A which is the transmission place of the attribute certificate issue request message 2251, Terminal B requires a public key certificate of Terminal A by transmitting the public key certificate demand message 2231 (223). The frame structure 1870 of this public key certificate demand message 2231 is as drawing 16 , and is the same as that of the frame 820 (drawing 9) of the attribute certificate issue proposal message 1032 explained in the 1st example of drawing 7 . However, a public key certificate is not contained in the payload section 1872.

[0086]

The terminal A which received the public key certificate demand message 2231 (123) transmits the public key certificate in the end of a local currently held on the generation key table 650 (drawing 1) by the public key certificate demand response message 1242 (124). Thereby, Terminal B receives the public key certificate of the terminal A which is an attribute certificate issue terminal (224). In addition, the frame structure 1880 of this public key certificate demand response message 1242 is as drawing 17 , and is the same as that of the frame 820 (drawing 9) of the attribute certificate issue proposal message 1032 explained in the 1st example of drawing 7 . The same is said of the point that the public key certificate 1889 of the terminal A which is a transmitting agency terminal as data of the payload section 1882 is contained.

[0087]

Terminal A will check Terminal B from the contents, if the attribute certificate issue request message 2251 transmitted from Terminal B is received (125). For example, decision whether it is the terminal which he can trust is demanded from a user by displaying the owner 716 (drawing 3) of the public key in the starting point terminal identification child 833 (drawing 9) and the public key certificate 8391 of the attribute certificate issue request frame 830 on a display 340 (drawing 1). If it is the terminal which the terminal B of a transmitting agency trusts, a user will perform confirmation operation by the control unit 350 (drawing 1).

[0088]

If a check is made by the user, Terminal A will transmit the attribute certificate issue message 1262 to Terminal B, in order to publish an attribute certificate (126). Thereby, Terminal B receives an attribute certificate (226). In addition, the frame structure 860 of this attribute certificate issue message 1262 is as drawing 11 having explained.

[0089]
Drawing 18 is drawing showing the procedure of the mutual recognition in the gestalt of operation of this invention. Mutual recognition is performed when the terminals which finished initial registration verify a mutual attribute certificate. In the wireless ad hoc communication system in the gestalt of operation of this invention, each terminal transmits a beacon periodically and tells existence of self to other terminals. Although it assumes below that it is that to which Terminal A gives an authentication demand by making the beacon of Terminal B into a trigger, it is [that authentication should finally just be performed mutually] good also considering the beacon of which terminal as a trigger.
[0090]
First, a beacon 2111 is transmitted in order that Terminal B may enter into a network (211). The frame structure of this beacon 2111 is as above-mentioned drawing 8 . Since Terminal B has the attribute certificate in the mutual recognition of this drawing 18 unlike the initial registration sequence of drawing 7 , the purport "which it has" is shown in the existence 818 of this attribute certificate.
[0091]
Terminal A will check the existence 818 of the attribute certificate of the beacon frame 810, if the beacon 2111 transmitted from Terminal B is received (111). If it judges that Terminal B has the attribute certificate, Terminal A will transmit the authentication demand message 1122 so that Terminal A may be attested to Terminal B (112). The frame structure of this authentication demand message 1122 is as drawing 19 . The authentication demand frame 870 consists of a header unit 871 and the payload section 872. A header unit 871 includes the starting point terminal identification child 873, the terminal point terminal identification child 874, the transmit-terminal identifier 875, received terminal identification 876, and the frame classification 877. About the contents in these header units 871, it is the same as that of the attribute certificate issue proposal frame 820 explained by drawing 9 . Moreover, with this authentication demand frame 870, the public key certificate 8791 and the attribute certificate 8792 of Terminal A which are a transmitting agency are contained as data 879 of the payload section 872. The public key certificate 8791 of Terminal A is beforehand stored in the generation key table 650 of Terminal A, and the attribute certificate 8792 of Terminal A is beforehand stored in the attribute certificate table 620 of Terminal A.
[0092]
Terminal B will attest Terminal A from the contents, if the authentication demand message 1122 transmitted from Terminal A is received (212). The public key of an attribute certificate authority is extracted from the public key certificate 612 (drawing 2) of the attribute certificate issue terminal list table 610, and, specifically, the message digest at the time of a signature is obtained by decoding the signature 729 (drawing 4) of the attribute certificate 8792 contained in the authentication

demand message 1122 with this public key. And the message digest of the attribute certification information 721 (drawing 4) on the attribute certificate 8792 is newly generated. It checks that this newly generated message digest is in agreement with the message digest at the time of a signature. Supposing these are not in agreement, the attribute certificate may have been altered after the signature and verification of an attribute certificate will be failing. When both are in agreement, the owner public key certificate identifier 723 (drawing 4) of the attribute certificate 8792 further contained in the authentication demand message 1122 checks that it is in agreement with the publisher 714 and serial number 712 (drawing 3) of the public key certificate 8791 which are contained in the authentication demand message 1122. If this is in agreement, it can check that the terminal A which is the owner of a public key certificate is the owner of an attribute certificate. Supposing these are not in agreement, in the owner of an attribute certificate, verification of the attribute certificate instead of Terminal A will be failing.

[0093]

In addition, it is necessary to check that that attribute certificate is not contained in the attribute certificate lapse list table 630 in the case of verification of this attribute certificate. When the publisher 724 and serial number 722 (drawing 4) of the attribute certificate 8792 are contained in the attribute certificate identifier 631 (drawing 5) of the attribute certificate lapse list table 630, the attribute certificate 8792 will be invalidated bordering on the lapse time of day 632. Therefore, verification of an attribute certificate is failing in that case.

[0094]

If it succeeds in authentication (212) of Terminal A, the authentication success message 2131 which notifies that Terminal B succeeded in authentication of Terminal A will be transmitted to Terminal A (213). The authentication response frame structure of this authentication success message 2131 is as drawing 20 . The authentication response frame 880 consists of a header unit 881 and the payload section 882. A header unit 881 includes the starting point terminal identification child 883, the terminal point terminal identification child 884, the transmit-terminal identifier 885, received terminal identification 886, and the frame classification 887. About the contents in these header units 881, it is the same as that of the attribute certificate issue proposal frame 820 explained by drawing 9 . In the case of the authentication success message 2131, the frame classification 887 serves as an authentication success frame. At this authentication response frame 880, although the reason classification 888 for a response is included further, in an authentication success, there is especially no need.

[0095]

In addition, when verification (212) of the attribute certificate of Terminal A goes wrong, the authentication failure message which notifies that Terminal B succeeded in authentication of Terminal A will be transmitted to Terminal A. The authentication

response frame structure of this authentication failure message is as drawing 20 having explained. However, in the case of an authentication failure message, the frame classification 887 serves as an authentication failure frame, and as a reason which failed in authentication, the reasons of the message digest inequality of an attribute certificate, an attribute certificate lapse, etc. are coded by the reason classification 888 for a response, and it is shown in it. These. The authentication success message 2131 or an authentication failure message is received and checked in Terminal A (113).

[0096]

If it succeeds in verification (212) of the attribute certificate of Terminal A, Terminal B will transmit the authentication demand message 2141 further so that Terminal B may be attested to Terminal A (214). The frame structure of this authentication demand message 2141 is the same as that of above-mentioned drawing 19 , and the public key certificate 8791 and the attribute certificate 8792 of Terminal B which are a transmitting agency are contained.

[0097]

Terminal A will attest Terminal B from the contents, if the authentication demand message 2141 transmitted from Terminal B is received (114). The contents of this authentication are as having already explained, and perform verification of an attribute certificate, a check of the owner of an attribute certificate, the check of the attribute certificate lapse list table 630, etc.

[0098]

If it succeeds in authentication (212) of Terminal B, the authentication success message 1152 which notifies that Terminal A succeeded in authentication of Terminal B will be transmitted to Terminal B (115). The authentication response frame structure of this authentication success message 1152 is the same as that of above-mentioned drawing 20 . Moreover, when verification (212) of the attribute certificate of Terminal B goes wrong, the authentication failure message which notifies that Terminal A succeeded in authentication of Terminal B will be transmitted to Terminal B. It is as drawing 20 having also explained the authentication response frame structure of this authentication failure message. These authentication success message 1152 or an authentication failure message is received and checked in Terminal B (215).

[0099]

Thus, mutual recognition will be completed if it succeeds in authentication of a mutual terminal in Terminal A and Terminal B. After this mutual recognition is completed, the contents of the attribute certificate issue terminal list table 610 and the attribute certificate lapse list table 630 are exchanged and merged mutually. Moreover, the terminal which newly turned into an attribute certificate issue terminal carries out broadcasting distribution of the public key certificate of self at all terminals. Furthermore, the terminal which published the attribute certificate lapse list carries

out broadcasting distribution of the attribute certificate lapse list as mentioned above at other terminals. The identity of the contents of the attribute certificate issue terminal list table 610 of each terminal under connection with a network and the attribute certificate lapse list table 630 is maintained by these.

[0100]

Next, with reference to a drawing, it explains that processing of each terminal of the wireless ad hoc communication system in the gestalt of operation of this invention flows.

[0101]

Drawing 21 is drawing showing the flow of processing of the attribute certificate issue terminal in the 1st example of initial registration of drawing 7 . First, if a beacon is received from other terminals, it will judge whether the beacon shows the purport in which the transmitting agency terminal of the beacon has the attribute certificate (step S911). If that beacon shows the purport which has the attribute certificate, since it is not necessary to publish an attribute certificate, it ends without performing processing of this initial registration. If the beacon does not show the purport which has the attribute certificate, it proposes checking the starting point terminal identification child of a beacon, and requesting issue of an attribute certificate to a transmitting agency terminal (step S912).

[0102]

Then, if there is an issue request of an attribute certificate (step S913), the information about a request former terminal will be displayed, and a check will be urged (step S914). Consequently, when checked as a terminal which can trust a requesting agency terminal, an attribute certificate is published to (step S915) and a requesting agency terminal (step S916). On the contrary, when a check is refused, refusal of an attribute certificate issue request is notified to a requesting agency terminal (step S917).

[0103]

Drawing 22 is drawing showing the flow of processing of the new-comer terminal in the 1st example of initial registration of drawing 7 . First, the beacon in which the purport which does not have the attribute certificate is shown is transmitted (step S921). Then, if there is an attribute certificate issue proposal from other terminals which answered the beacon (step S922), the check of the terminal which made the proposal will be demanded from a user (step S923). If it is the terminal which the terminal of a transmitting agency trusts, the check which means that I have the terminal publish an attribute certificate will be made (step S924). If this check is made, an issue request of an attribute certificate will be performed to a that transmitting former terminal (step S925). Thereby, issue of an attribute certificate can be received (step S926). On the other hand, if this check is not carried out, processing of initial registration is not completed, and an attribute certificate is not published.

[0104]

Drawing 23 is drawing showing the flow of processing of the attribute certificate issue terminal in the modification of the 1st example of initial registration of drawing 12 . First, if a beacon is received from other terminals, it will judge whether the beacon shows the purport in which the transmitting agency terminal of the beacon has the attribute certificate (step S971). If that beacon shows the purport which has the attribute certificate, since it is not necessary to publish an attribute certificate, it ends without performing processing of this initial registration. If the beacon does not show the purport which has the attribute certificate, the starting point terminal identification child of a beacon is checked, and an attribute certificate is published to a transmitting agency terminal (step S972), and the attribute certificate is included in a proposal message, and it transmits (step S973).

[0105]

Drawing 24 is drawing showing the flow of processing of the new-comer terminal in the modification of the 1st example of initial registration of drawing 12 . First, the beacon in which the purport which does not have the attribute certificate is shown is transmitted (step S981). Then, if there is an attribute certificate issue proposal from other terminals which answered the beacon (step S982), the check (step S983) of the terminal which made the proposal will be demanded from a user. If it is the terminal which the terminal of a transmitting agency trusts (step S984), the message which shows the purport which received the attribute certificate which the terminal published (step S985), and received the attribute certificate will be transmitted to the terminal of a transmitting agency (step S986).

[0106]

Drawing 25 is drawing showing the flow of processing of the new-comer terminal in the 2nd example of initial registration of drawing 15 . First, the starting point terminal identification child 813 (drawing 8) of a beacon who received is grasped, and it judges whether issue of an attribute certificate is requested from the transmitting agency terminal of the beacon (step S951). It ends the processing concerned, in not wishing to publish. When the new-comer terminal does not possess the public key certificate of a beacon transmitting former terminal, a public key certificate is required and (step S953) received to (step S952) beacon transmitting former terminal (step S954).

[0107]

And the public key contained in a public key certificate is the thing of a beacon transmitting former terminal, and when it judges that I have the terminal concerned publish an attribute certificate, an issue request of an attribute certificate is performed to (step S955) and a transmitting former terminal (step S956). Thereby, issue of an attribute certificate can be received. On the other hand, when it cannot be checked that a public key is the thing of a beacon transmitting former terminal, an issue request of an attribute certificate is not performed.

[0108]

Drawing 26 is drawing showing the flow of processing of the attribute certificate issue terminal in the 2nd example of initial registration of drawing 15 . First, if there is a demand of a public key certificate from other terminals (step S961), a demand will be answered and a public key certificate will be transmitted (step S962). Then, if there is an issue request of an attribute certificate (step S963), the information about a request former terminal will be displayed, and a check will be urged (step S964). Consequently, when checked as a terminal which can trust a requesting agency terminal, an attribute certificate is published to (step S965) and a requesting agency terminal (step S966). On the contrary, when a check is refused, refusal of an attribute certificate issue request is notified to a requesting agency terminal (step S967).

[0109]

Drawing 27 is drawing showing the flow of processing of the beacon accepting station in the mutual recognition of drawing 18 . First, if a beacon is received from other terminals, it will judge whether the beacon shows the purport in which the transmit terminal of the beacon has the attribute certificate (step S931). If that beacon does not show the purport which has the attribute certificate, since mutual recognition cannot be performed, it ends without performing processing of this mutual recognition. In addition, the proposal of attribute certificate issue is made from an attribute certificate issue terminal in this case. On the other hand, if the beacon shows the purport which has the attribute certificate, an authentication demand will be transmitted to the transmit terminal of a beacon (step S932). Consequently, if authentication goes wrong in the transmit terminal of a beacon, it cannot complete (step S933) and this mutual recognition cannot constitute a network mutually the end of both ends. On the other hand, if authentication succeeds in the transmit terminal of a beacon, an authentication demand will be transmitted from a beacon transmit terminal on the contrary.

[0110]

Reception of an authentication demand attests the beacon transmit terminal of authentication demand origin (step S935). (step S934) If it succeeds in authentication (step S936), the purport of an authentication success will be transmitted to an authentication demand terminal (beacon transmit terminal) (step S937). On the other hand, when authentication goes wrong, the purport of (step S936) and authentication failure is transmitted to an authentication demand terminal (step S938).

[0111]

Drawing 28 is drawing showing the flow of processing of the beacon transmit terminal in the mutual recognition of drawing 18 . First, the beacon in which the purport which has the attribute certificate is shown is transmitted (step S941). Then, reception of the authentication demand from other terminals which answered the beacon attests the beacon accepting station of authentication demand origin (step S943). (step S942) When authentication goes wrong, the purport of (step S944) and authentication failure is transmitted to an authentication demand terminal (beacon accepting station) (step

S945). On the other hand, when it succeeds in authentication, while transmitting the purport of (step S944) and an authentication success to an authentication demand terminal (step S946), an authentication demand is transmitted to a beacon accepting station (step S947). Then, the response to an authentication demand is transmitted from a beacon accepting station (step S948).

[0112]

Next, the connection relation between the terminals of the wireless ad hoc communication system in the gestalt of operation of this invention is explained with reference to a drawing.

[0113]

Drawing 29 is drawing showing the process in which terminals constitute the network of wireless ad hoc communication system. Supposing Terminal A (100) is functioning as an attribute certificate issue terminal first, the public key certificate (PK-A) of Terminal A will be held at the attribute certificate issue terminal list table 610 of Terminal A, and the attribute certificate (AC-A) of terminal A issue will be held at the attribute certificate table of Terminal A (drawing 29 (a)). If Terminal B (200) transmits a beacon, an attribute certificate is published from Terminal A to Terminal B, as a result of initial registration, the public key certificate (PK-A) of Terminal A will be held at the attribute certificate issue terminal list table 610 of Terminal B, and the attribute certificate (AC-A) of terminal A issue will be held at the attribute certificate table of Terminal B (drawing 29 (b)). Terminal A and Terminal B constitute the network of wireless ad hoc communication system by performing mutual recognition after initial registration.

[0114]

Then, if Terminal C transmits a beacon, an attribute certificate will be published from Terminal A to Terminal C through Terminal B, and Terminal C will enter into the network of wireless ad hoc communication system by performing Terminal B and mutual recognition after initial registration (drawing 29 (c)). Furthermore, also when Terminal C transmits a beacon, Terminal D enters into the network of wireless ad hoc communication system through the same procedure (drawing 29 (c)).

[0115]

And when the terminal A which was functioning as an attribute certificate issue terminal until now is cut from a network by a certain factor, other terminals will function as an attribute certificate issue terminal. Although various things can be considered as a selection criterion of this attribute certificate issue terminal, the terminal which exists in the center position at a certain time, a terminal with most remaining capacity of a cell, etc. can be chosen, for example. For example, supposing Terminal B is chosen as an attribute certificate issue terminal, Terminal B will carry out broadcasting distribution at all terminals while connecting the public key certificate (PK-B) of self. Each terminal stores the public key certificate (PK-B) of Terminal B in the attribute certificate issue terminal list table 610 with the terminal

identification child of Terminal B (drawing 29 (d)).
[0116]
Drawing 30 is drawing showing the process in which the once cut terminal enters into the network of wireless ad hoc communication system again. If Terminal E transmits a beacon after Terminal A is cut and Terminal B comes to function as an attribute certificate issue terminal (drawing 30 (a)), an attribute certificate will be published from Terminal B to Terminal E. The public key certificate (PK-B) of the terminal B which is the present attribute certificate issue terminal, and the public key certificate (PK-A) of the terminal A which is the past attribute certificate issue terminal are held at the attribute certificate issue terminal list table 610 of Terminal E as a result of initial registration. Moreover, the attribute certificate (AC-B) of terminal B issue is held at the attribute certificate table of Terminal E (drawing 30 (b)).
[0117]
Then, when Terminal A connects again, Terminal A attests with the attribute certificate (AC-A) by the terminal A issue currently held. And the attribute certificate issue terminal list table 610 is updated between Terminals B after mutual recognition. Consequently, the public key certificate (PK-B) of Terminal B is newly held at the attribute certificate issue terminal list table 610 of Terminal A (drawing 30 (c)).
[0118]
Thus, according to the gestalt of operation of this invention, the attribute certificate issue terminal which received the beacon checks the existence 818 (drawing 8) of the attribute certificate of the beacon frame 810. When it is judged that the beacon transmit terminal does not have the attribute certificate By transmitting the attribute certificate issue proposal frame 820 (drawing 9) which proposes an issue request of an attribute certificate to a beacon transmit terminal, ignited by these, autonomous distribution can be carried out and an attribute certificate can be published.
[0119]
In addition, the gestalt of operation of this invention is illustrated, and this invention is not restricted to this but can perform various deformation here in the range which does not deviate from the summary of this invention.
[0120]
Moreover, the procedure explained here may be regarded as an approach of having the procedure of these single strings, and may be regarded as a record medium which memorizes the program thru/or its program for making a computer (terminal) perform the procedure of these single strings.
[Availability on industry]
[0121]
This invention can be applied in case a terminal authority authentication certificate is published between the terminals for example, in wireless ad hoc communication system as an example of an activity of this invention.
[Brief Description of the Drawings]

[0122]
[Drawing 1] It is drawing showing the example of a configuration of the wireless terminal 300 used in the wireless ad hoc communication system in the gestalt of operation of this invention.
[Drawing 2] It is the example of a configuration of the attribute certificate issue terminal list table 610 in the gestalt of operation of this invention.
[Drawing 3] It is drawing showing the format 710 of the public key certificate 612 held at the attribute certificate issue terminal list table 610 in the gestalt of operation of this invention.
[Drawing 4] It is drawing showing the format 720 of the attribute certificate held at the attribute certificate table 620 in the gestalt of operation of this invention.
[Drawing 5] It is the example of a configuration of the attribute certificate lapse list table 630 in the gestalt of operation of this invention.
[Drawing 6] It is drawing showing a format of the attribute certificate lapse list 730 in the gestalt of operation of this invention.
[Drawing 7] It is drawing showing the 1st example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 8] It is drawing showing the configuration of the beacon frame 810 in the gestalt of operation of this invention.
[Drawing 9] It is drawing showing the configuration of the attribute certificate issue proposal frame 820 in the gestalt of operation of this invention, and the attribute certificate issue request frame 830.
[Drawing 10] It is drawing showing the configuration of the attribute certificate issue proposal refusal frame 840 in the gestalt of operation of this invention, and the attribute certificate issue request refusal frame 850.
[Drawing 11] It is drawing showing the configuration of the attribute certificate issue frame 860 in the gestalt of operation of this invention.
[Drawing 12] It is drawing showing the modification of the 1st example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 13] It is drawing showing the configuration of the attribute certificate issue proposal frame 1820 in the gestalt of operation of this invention.
[Drawing 14] It is drawing showing the configuration of the attribute certificate issue proposal receipt frame 1830 in the gestalt of operation of this invention.
[Drawing 15] It is drawing showing the 2nd example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 16] It is drawing showing the configuration of the public key certificate demand frame 870 in the gestalt of operation of this invention.
[Drawing 17] It is drawing showing the configuration of the public key certificate demand response frame 880 in the gestalt of operation of this invention.
[Drawing 18] It is drawing showing the procedure of the mutual recognition in the gestalt of operation of this invention.

[Drawing 19] It is drawing showing the configuration of the authentication demand frame 870 in the gestalt of operation of this invention.
[Drawing 20] It is drawing showing the configuration of the authentication response frame 880 in the gestalt of operation of this invention.
[Drawing 21] It is drawing showing the flow of the processing in the 1st example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 22] It is drawing showing the flow of the processing in the 1st example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 23] It is drawing showing the flow of the processing in the modification of the 1st example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 24] It is drawing showing the flow of the processing in the modification of the 1st example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 25] It is drawing showing the flow of the processing in the 2nd example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 26] It is drawing showing the flow of the processing in the 2nd example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 27] It is drawing showing the flow of processing of the beacon accepting station in the case of the mutual recognition in the gestalt of operation of this invention.
[Drawing 28] It is drawing showing the flow of processing of the beacon transmit terminal in the case of the mutual recognition in the gestalt of operation of this invention.
[Drawing 29] It is drawing showing the process in which terminals constitute the network of wireless ad hoc communication system in the gestalt of operation of this invention.
[Drawing 30] It is drawing showing the process in which the terminal once cut in the gestalt of operation of this invention enters into the network of wireless ad hoc communication system again.
[Description of Notations]
[0123]
300 Wireless Terminal
310 Antenna
320 Communications Processing Section
330 Control Section
340 Display

350 Control Unit
360 Loudspeaker
370 Microphone
380 Bus
600 Memory
610 Attribute Certificate Issue Terminal List Table
620 Attribute Certificate Table
630 Attribute Certificate Lapse List Table
650 Generation Key Table
710 Public Key Certificate
720 Attribute Certificate
730 Attribute Certificate Lapse List
810 Beacon Frame
820 Attribute Certificate Issue Proposal Frame
830 Attribute Certificate Issue Request Frame
840 Attribute Certificate Issue Proposal Refusal Frame
850 Attribute Certificate Issue Request Refusal Frame
860 Attribute Certificate Issue Frame
870 Authentication Demand Frame
880 Authentication Response Frame
1820 Attribute Certificate Issue Proposal Frame
1830 Attribute Certificate Issue Proposal Receipt Frame
1870 Public Key Certificate Demand Frame
1880 Public Key Certificate Demand Response Frame

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[0122]

[Drawing 1] It is drawing showing the example of a configuration of the wireless terminal 300 used in the wireless ad hoc communication system in the gestalt of operation of this invention.

[Drawing 2] It is the example of a configuration of the attribute certificate issue terminal list table 610 in the gestalt of operation of this invention.

[Drawing 3] It is drawing showing the format 710 of the public key certificate 612 held at the attribute certificate issue terminal list table 610 in the gestalt of operation of this invention.

[Drawing 4] It is drawing showing the format 720 of the attribute certificate held at

the attribute certificate table 620 in the gestalt of operation of this invention.
[Drawing 5] It is the example of a configuration of the attribute certificate lapse list table 630 in the gestalt of operation of this invention.
[Drawing 6] It is drawing showing a format of the attribute certificate lapse list 730 in the gestalt of operation of this invention.
[Drawing 7] It is drawing showing the 1st example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 8] It is drawing showing the configuration of the beacon frame 810 in the gestalt of operation of this invention.
[Drawing 9] It is drawing showing the configuration of the attribute certificate issue proposal frame 820 in the gestalt of operation of this invention, and the attribute certificate issue request frame 830.
[Drawing 10] It is drawing showing the configuration of the attribute certificate issue proposal refusal frame 840 in the gestalt of operation of this invention, and the attribute certificate issue request refusal frame 850.
[Drawing 11] It is drawing showing the configuration of the attribute certificate issue frame 860 in the gestalt of operation of this invention.
[Drawing 12] It is drawing showing the modification of the 1st example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 13] It is drawing showing the configuration of the attribute certificate issue proposal frame 1820 in the gestalt of operation of this invention.
[Drawing 14] It is drawing showing the configuration of the attribute certificate issue proposal receipt frame 1830 in the gestalt of operation of this invention.
[Drawing 15] It is drawing showing the 2nd example of the procedure of the initial registration in the gestalt of operation of this invention.
[Drawing 16] It is drawing showing the configuration of the public key certificate demand frame 870 in the gestalt of operation of this invention.
[Drawing 17] It is drawing showing the configuration of the public key certificate demand response frame 880 in the gestalt of operation of this invention.
[Drawing 18] It is drawing showing the procedure of the mutual recognition in the gestalt of operation of this invention.
[Drawing 19] It is drawing showing the configuration of the authentication demand frame 870 in the gestalt of operation of this invention.
[Drawing 20] It is drawing showing the configuration of the authentication response frame 880 in the gestalt of operation of this invention.
[Drawing 21] It is drawing showing the flow of the processing in the 1st example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 22] It is drawing showing the flow of the processing in the 1st example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.

[Drawing 23] It is drawing showing the flow of the processing in the modification of the 1st example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 24] It is drawing showing the flow of the processing in the modification of the 1st example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 25] It is drawing showing the flow of the processing in the 2nd example of the new-comer terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 26] It is drawing showing the flow of the processing in the 2nd example of the attribute certificate issue terminal in the case of the initial registration in the gestalt of operation of this invention.
[Drawing 27] It is drawing showing the flow of processing of the beacon accepting station in the case of the mutual recognition in the gestalt of operation of this invention.
[Drawing 28] It is drawing showing the flow of processing of the beacon transmit terminal in the case of the mutual recognition in the gestalt of operation of this invention.
[Drawing 29] It is drawing showing the process in which terminals constitute the network of wireless ad hoc communication system in the gestalt of operation of this invention.
[Drawing 30] It is drawing showing the process in which the terminal once cut in the gestalt of operation of this invention enters into the network of wireless ad hoc communication system again.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-260803
(P2004-260803A)
(43)公開日　平成16年9月16日(2004.9.16)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675Z	5J104
G09C	1/00	G09C	1/00	640E	5K033
H04L	12/28	H04L	12/28	307	5K067
H04Q	7/38	H04B	7/26	109R	

審査請求 未請求　請求項の数 39　ＯＬ　（全 35 頁）

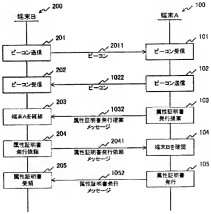
(21)出願番号　特願2004-15193(P2004-15193)
(22)出願日　平成16年1月23日(2004.1.23)
(31)優先権主張番号　特願2003-26544(P2003-26544)
(32)優先日　平成15年2月3日(2003.2.3)
(33)優先権主張国　日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100112955
弁理士　丸島　敏一
(72)発明者　鈴木　英之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5J104 AA07 KA02 KA05 KA06 NA02 NA38 PA01
5K033 AA08 CC01 DA17 DB16 DB18 EA05 EC02
5K067 AA30 DD17 EE02 HH22 HH23 HH24 HH31 JJ61

(54)【発明の名称】無線アドホック通信システム、端末、その端末における属性証明書発行提案方法及び属性証明書発行依頼方法並びにそれらの方法を端末に実行させるためのプログラム

(57)【要約】
【課題】　無線アドホック通信システムにおいて、属性証明書の発行を自律分散して行う。
【解決手段】　端末Ｂ２００は無線アドホック通信システムのネットワークに参入するためにビーコン２０１１を送信する。このビーコン２０１１には、端末Ｂ２００が属性証明書を有しているか否かが示されている。ビーコン２０１１を受けた端末Ａ１００は、ビーコンをチェックして、端末Ｂ２００が属性証明書を有していないと判断すると、属性証明書の発行を依頼するよう端末Ｂ２００に対して提案する属性証明書発行提案メッセージ１０３２を送信する。これに応答して、端末Ｂ２００が属性証明書発行依頼メッセージ２０４１を送信すると、端末Ａ１００は属性証明書発行メッセージ１０５２を端末Ｂ２００に送信する。
【選択図】　図７



【特許請求の範囲】
【請求項１】
複数の端末により構成される無線アドホック通信システムであって、
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する第１の端末と、
前記信号に応答して端末権限認証証明書発行依頼をするよう前記第１の端末に対して提案する第２の端末と
を具備する無線アドホック通信システム。
【請求項２】
ビーコン情報を含む信号を受信する受信手段と、
この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると端末権限認証証明書発行依頼をするよう当該他の端末に対して提案する端末権限認証証明書発行提案手段と
を具備することを特徴とする端末。
【請求項３】
前記受信手段が受信した前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、
前記端末権限認証証明書発行提案手段は、前記端末識別情報に基づいて前記提案を行うことを特徴とする請求項２記載の端末。
【請求項４】
前記端末権限認証証明書発行提案手段は、前記他の端末に対して前記端末権限認証証明書発行依頼を提案する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項２記載の端末。
【請求項５】
ビーコン情報を含む信号を受信する受信手段と、
この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると当該他の端末を所有者とする端末権限認証証明書を発行して当該他の端末に対して提案する端末権限認証証明書発行提案手段と
を具備することを特徴とする端末。
【請求項６】
前記受信手段が受信した前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、
前記端末権限認証証明書発行提案手段は、前記端末識別情報に基づいて前記提案を行うことを特徴とする請求項５記載の端末。
【請求項７】
前記端末権限認証証明書発行提案手段は、前記他の端末に対して前記端末権限認証証明書発行依頼を提案する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項５記載の端末。
【請求項８】
ビーコン情報を含む信号を受信するための受信手段と、
この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末が端末権限認証証明書を有する旨を前記信号が示していなければ端末権限認証証明書発行依頼をするよう当該他の端末に対して提案する端末権限認証証明書発行提案手段と
を具備することを特徴とする端末。
【請求項９】
前記受信手段が受信した前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、
前記端末権限認証証明書発行提案手段は、前記端末識別情報に基づいて前記提案を行うことを特徴とする請求項８記載の端末。
【請求項１０】

前記端末権限認証証明書発行提案手段は、前記他の端末に対して前記端末権限認証証明書発行依頼を提案する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項８記載の端末。
【請求項１１】
端末権限認証証明書発行依頼を受信するための端末権限認証証明書発行依頼受信手段と、
この端末権限認証証明書発行依頼受信手段が前記他の端末から端末権限認証証明書発行依頼を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、
前記確認がなされた場合には前記他の端末に対して端末権限認証証明書を発行し、前記確認が拒否された場合には前記他の端末に対して端末権限認証証明書発行依頼の拒否を通知する端末権限認証証明書発行手段と
をさらに具備することを特徴とする請求項１０記載の端末。
【請求項１２】
端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルをさらに具備し、
前記端末権限認証証明書発行手段は、前記端末権限認証証明書の発行に際して前記端末権限認証証明書発行端末リストテーブルに保持された前記端末権限認証証明書発行端末の公開鍵証明書を前記他の端末に送信する
ことを特徴とする請求項１１記載の端末。
【請求項１３】
端末権限認証証明書の失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、
前記端末権限認証証明書発行手段は、前記端末権限認証証明書の発行に際して前記端末権限認証証明書失効リストテーブルに保持された前記端末権限認証証明書失効リストを前記他の端末に送信する
ことを特徴とする請求項１１記載の端末。
【請求項１４】
ビーコン情報を含む信号を受信するための受信手段と、
この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末が端末権限認証証明書を有する旨を前記信号が示していなければ当該他の端末を所有者とする端末権限認証証明書を発行して当該他の端末に対して提案する端末権限認証証明書発行提案手段と
を具備することを特徴とする端末。
【請求項１５】
前記受信手段が受信した前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、
前記端末権限認証証明書発行提案手段は、前記端末識別情報に基づいて前記提案を行うことを特徴とする請求項１４記載の端末。
【請求項１６】
前記端末権限認証証明書発行提案手段は、前記他の端末に対して前記端末権限認証証明書発行依頼を提案する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項１４記載の端末。
【請求項１７】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する送信手段と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する端末権限認証証明書発行提案受信手段と、
この端末権限認証証明書発行提案受信手段が他の端末から前記提案を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、
前記確認がなされた場合には前記他の端末に対して端末権限認証証明書の発行を依頼し

、前記確認が拒否された場合には前記他の端末に対して端末権限認証証明書発行提案の拒否を通知する端末権限認証証明書発行依頼手段と
を具備する端末。
【請求項１８】
前記端末権限認証証明書発行依頼手段は、前記他の端末に対して前記端末権限認証証明書発行を依頼する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項１７記載の端末。
【請求項１９】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する送信手段と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する端末権限認証証明書発行提案受信手段と、
この端末権限認証証明書発行提案受信手段が他の端末から前記提案を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、
前記確認がなされると、前記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、前記提案が発行済みの端末権限認証証明書を含んでいない場合には前記他の端末に対して端末権限認証証明書の発行を依頼する端末権限認証証明書発行依頼手段と
を具備する端末。
【請求項２０】
前記端末権限認証証明書発行依頼手段は、前記他の端末に対して前記端末権限認証証明書発行を依頼する際に前記端末の公開鍵証明書を併せて提示する
ことを特徴とする請求項１９記載の端末。
【請求項２１】
ビーコン情報を含む信号を受信する受信手段と、
この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると端末権限認証証明書発行をするよう前記他の端末に対して依頼する端末権限認証証明書発行依頼手段と
を具備することを特徴とする端末。
【請求項２２】
前記受信手段が受信した前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、
端末権限認証証明書発行依頼手段は、前記端末識別情報に基づいて前記提案を行う
ことを特徴とする請求項２１記載の端末。
【請求項２３】
自端末のアクセス権限を示す第１の端末権限認証証明書を保持する端末権限認証証明書テーブルと、
ビーコン情報を含む信号を受信するための受信手段と、
この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末のアクセス権限を示す第２の端末権限認証証明書を当該他の端末が有する旨を前記信号が示していれば前記端末権限認証証明書テーブルに保持された前記第１の端末権限認証証明書を提示して前記他の端末に対して前記自端末の認証を要求する認証要求手段と
を具備することを特徴とする端末。
【請求項２４】
端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、
前記認証要求手段による認証要求に応答して前記他の端末が要求する第２の認証要求を受信する認証要求受信手段と、
この認証要求受信手段が受信した前記第２の認証要求に含まれる前記第２の端末権限認証証明書を前記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と

をさらに具備することを特徴とする請求項２３記載の端末。
【請求項２５】
端末権限認証証明書失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、
前記検証手段は、前記端末権限認証証明書失効リストテーブルに保持される前記端末権限認証証明書失効リストにおいて前記第２の端末権限認証証明書が失効している場合には認証失敗との判断を行う
ことを特徴とする請求項２４記載の端末。
【請求項２６】
端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、
第１の端末権限認証証明書を有する他の端末に対して第２の端末権限認証証明書を有する旨を示すビーコン情報を含む信号を送信する送信手段と、
自端末のアクセス権限を示す前記第２の端末権限認証証明書を保持する端末権限認証証明書テーブルと、
前記信号に対する他の端末からの第１の認証要求を受信する認証要求受信手段と、
この認証要求受信手段が受信した前記第１の認証要求に含まれる前記第１の端末権限認証証明書を前記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、
この検証手段において認証が成功すると前記他の端末に対して前記端末権限認証証明書テーブルに保持された前記第２の端末権限認証証明書を提示して前記他の端末に対して前記自端末の認証を要求する第２の認証要求を行う認証要求手段と
を具備することを特徴とする端末。
【請求項２７】
端末権限認証証明書失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、
前記検証手段は、前記端末権限認証証明書失効リストテーブルに保持される前記端末権限認証証明書失効リストにおいて前記第２の端末権限認証証明書が失効している場合には認証失敗との判断を行う
ことを特徴とする請求項２６記載の端末。
【請求項２８】
ビーコン情報を含む信号を受信する手順と、
前記信号の送信元端末が端末権限認証証明書を有する旨を前記信号が示していなければ端末権限認証証明書発行依頼をするよう前記送信元端末に対して提案する手順と
を具備することを特徴とする端末権限認証証明書発行提案方法。
【請求項２９】
前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手順をさらに具備し、
前記端末識別情報に基づいて前記提案を行う
ことを特徴とする請求項２８記載の端末権限認証証明書発行提案方法。
【請求項３０】
ビーコン情報を含む信号を受信する手順と、
前記信号の送信元端末が端末権限認証証明書を有する旨を前記信号が示していなければ当該送信元端末を所有者とする端末権限認証証明書を発行して当該送信元端末に対して提案する手順と
を具備することを特徴とする端末権限認証証明書発行提案方法。
【請求項３１】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、
前記提案の送信元端末に関する情報を表示して確認を促す手順と、

前記確認がなされた場合には前記送信元端末に対して端末権限認証証明書の発行を依頼し、前記確認が拒否された場合には前記送信元端末に対して端末権限認証証明書発行提案の拒否を通知する手順と
を具備する端末権限認証証明書発行依頼方法。
【請求項３２】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、
前記提案の送信元端末に関する情報を表示して確認を促す手順と、
前記確認がなされると、前記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、前記提案が発行済みの端末権限認証証明書を含んでいない場合には前記送信元端末に対して端末権限認証証明書の発行を依頼する手順と
を具備する端末権限認証証明書発行依頼方法。
【請求項３３】
ビーコン情報を含む信号を受信する手順と、
他の端末から前記信号を受信すると端末権限認証証明書発行をするよう当該他の端末に対して依頼する手順と
を具備することを特徴とする端末権限認証証明書発行依頼方法。
【請求項３４】
前記他の端末からの前記信号より当該他の端末の端末識別情報を取得する手順をさらに具備し、
前記端末識別情報に基づいて前記依頼を行う
ことを特徴とする請求項３３記載の端末権限認証証明書発行依頼方法。
【請求項３５】
ビーコン情報を含む信号を受信する手順と、
前記信号の送信元端末が端末権限認証証明書を有する旨を前記信号が示していなければ端末権限認証証明書発行依頼をするよう前記送信元端末に対して提案する手順と
を端末に実行させることを特徴とするプログラム。
【請求項３６】
ビーコン情報を含む信号を受信する手順と、
前記信号の送信元端末が端末権限認証証明書を有する旨を前記信号が示していなければ当該送信元端末を所有者とする端末権限認証証明書を発行して当該送信元端末に対して提案する手順と
を端末に実行させることを特徴とするプログラム。
【請求項３７】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、
前記提案の送信元端末に関する情報を表示して確認を促す手順と、
前記確認がなされた場合には前記送信元端末に対して端末権限認証証明書の発行を依頼し、前記確認が拒否された場合には前記送信元端末に対して端末権限認証証明書発行提案の拒否を通知する手順と
を端末に実行させることを特徴とするプログラム。
【請求項３８】
端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、
前記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、
前記提案の送信元端末に関する情報を表示して確認を促す手順と、
前記確認がなされると、前記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、前記提案が発行済みの端末権限認証証明書を含んでいない場合には前記送信元端末に対して端末権限認証証明書の発行を依頼する手順と
を端末に実行させることを特徴とするプログラム。
【請求項３９】

ビーコン情報を含む信号を受信する手順と、
他の端末から前記信号を受信すると端末権限認証証明書発行をするよう当該他の端末に対して依頼する手順と
を端末に実行させることを特徴とするプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線アドホック通信システムに関し、特に端末権限認証証明書を用いてネットワークへのアクセス権限を認証させる無線アドホック通信システム、当該システムにおける端末、および、これらにおける処理方法ならびに当該方法をコンピュータ（端末）に実行させるプログラムに関する。
【背景技術】
【０００２】
電子機器の小型化、高性能化が進み、簡単に持ち運び利用することが可能となったことから、必要になったその場で端末をネットワークに接続し、通信を可能とする環境が求められている。その一つとして、必要に応じて一時的に構築されるネットワーク、すなわち無線アドホックネットワーク技術の開発が進められている。この無線アドホックネットワークでは、特定のアクセスポイントを設けることなく、各端末（例えば、コンピュータ、携帯情報端末（ＰＤＡ：Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ）、携帯電話等）が自律分散して相互に接続される。
【０００３】
一般に、あるネットワーク資源に対して接続する権限を有しない機器がアクセスすることを防ぐために、端末権限認証証明書を利用した権限管理が行われている。この端末権限認証証明書の一例として、属性証明書が２０００年３月にＸ．５０９バージョン３により新たに定義され、２００２年４月より標準化過程の仕様書（Ｓｔａｎｄａｒｄ Ｔｒａｃｋ ＲＦＣ（Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ））としてプロファイル（属性証明書に含まれるデータフィールドの内容の定義）がまとめられている。属性証明書をネットワーク資源へのアクセス許可証として利用することにより、ネットワーク資源に接続する権限を確認し、接続資格を保有している端末だけに接続を許可することができる。なお、本明細書では、端末権限認証証明書の一例として属性証明書について説明するが、例えば、ＸＭＬ言語等により端末権限を記述しておき、権限を有する機関がそれに署名を付することにより作成されたようなものであっても本発明における端末権限認証証明書として機能し得る。
【０００４】
従来の通信システムにおいては、認証に用いられるデータはネットワーク上の特定の装置において集中管理されている。例えば、一つの公開鍵管理装置を複数の無線通信交換システムにより共有し、ある無線通信交換システムのサービスエリアに移動端末が移動すると公開鍵管理装置にその移動端末の公開鍵を要求する技術が提案されている（例えば、特許文献１参照。）。
【特許文献１】特開平１０－１１２８８３号公報（図１）
【発明の開示】
【発明が解決しようとする課題】
【０００５】
従来の通信システムでは認証に用いられるデータは集中管理されているが、無線アドホック通信システムにおいては端末は常に移動し、その時々によってネットワークを構成する端末が異なり、そのような集中管理を行う装置が常に存在するとは限らない。また、無線媒体の性質上、そのような集中管理を行う装置への通信路が常に確保されているとは限らないため、集中管理に適さない。
【０００６】

そこで、本発明の目的は、無線アドホック通信システムにおいて、端末権限認証証明書の発行を自律分散して行うことにある。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、ビーコン等）を送信する無線ネットワークにおいて有用である。

【課題を解決するための手段】

【０００７】

上記課題を解決するために本発明の請求項１記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する第１の端末と、上記信号に応答して端末権限認証証明書発行依頼をするよう上記第１の端末に対して提案する第２の端末とを具備する。これにより、第１の端末からの信号をトリガーとして第２の端末との間で端末権限認証証明書の発行処理を展開させるという作用をもたらす。

【０００８】

また、本発明の請求項２記載の端末は、ビーコン情報を含む信号を受信するための受信手段と、この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると端末権限認証証明書発行依頼をするよう当該他の端末に対して提案する端末権限認証証明書発行提案手段とを具備する。これにより、ビーコン情報を含む信号をトリガーとして端末権限認証証明書の発行処理を展開させるという作用をもたらす。

【０００９】

また、本発明の請求項３記載の端末は、請求項２記載の端末において、上記受信手段が受信した上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、上記端末権限認証証明書発行提案手段が上記端末識別情報に基づいて上記提案を行う。これにより、端末権限認証証明書発行依頼を提案すべき端末を確認した上で提案を行わせるという作用をもたらす。

【００１０】

また、本発明の請求項４記載の端末は、請求項２記載の端末において、上記端末権限認証証明書発行提案手段が上記他の端末に対して上記端末権限認証証明書発行依頼を提案する際に上記端末の公開鍵証明書を併せて提示するものである。これにより、端末権限認証証明書発行依頼の提案をした端末の本人性をビーコン情報を含む信号の送信端末に確認させるという作用をもたらす。

【００１１】

また、本発明の請求項５記載の端末は、ビーコン情報を含む信号を受信する受信手段と、この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると当該他の端末を所有者とする端末権限認証証明書を発行して当該他の端末に対して提案する端末権限認証証明書発行提案手段とを具備する。これにより、ビーコン情報を含む信号をトリガーとして、端末権限認証証明書発行依頼に先立って端末権限認証証明書を発行させるという作用をもたらす。

【００１２】

また、本発明の請求項６記載の端末は、請求項５記載の端末において、上記受信手段が受信した上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、上記端末権限認証証明書発行提案手段は、上記端末識別情報に基づいて上記提案を行う。これにより、端末権限認証証明書発行依頼を提案すべき端末を確認した上で端末権限認証証明書の受領を行わせるという作用をもたらす。

【００１３】

また、本発明の請求項７記載の端末は、請求項５記載の端末において、上記端末権限認証証明書発行提案手段が、上記他の端末に対して上記端末権限認証証明書発行依頼を提案する際に上記端末の公開鍵証明書を併せて提示するものである。これにより、端末権限認証証明書発行の提案をした端末の本人性をビーコン情報を含む信号の送信端末に確認させるという作用をもたらす。

【００１４】

また、本発明の請求項８記載の端末は、ビーコン情報を含む信号を受信するための受信手段と、この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末が端末権限認証証明書を有する旨を上記信号が示していなければ端末権限認証証明書発行依頼をするよう当該他の端末に対して提案する端末権限認証証明書発行提案手段とを具備する。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に当該信号をトリガーとして端末権限認証証明書の発行処理を展開させるという作用をもたらす。

【００１５】

また、本発明の請求項９記載の端末は、請求項８記載の端末において、上記受信手段が受信した上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、上記端末権限認証証明書発行提案手段は上記端末識別情報に基づいて上記提案を行うものである。これにより、端末権限認証証明書発行依頼を提案すべき端末を確認した上で提案を行わせるという作用をもたらす。

【００１６】

また、本発明の請求項１０記載の端末は、請求項８記載の端末において、上記端末権限認証証明書発行提案手段が、上記他の端末に対して上記端末権限認証証明書発行依頼を提案する際に上記端末の公開鍵証明書を併せて提示する。これにより、端末権限認証証明書発行依頼の提案をした端末の本人性をビーコン情報を含む信号の送信端末に確認させるという作用をもたらす。

【００１７】

また、本発明の請求項１１記載の端末は、請求項１０記載の端末において、端末権限認証証明書発行依頼を受信するための端末権限認証証明書発行依頼受信手段と、この端末権限認証証明書発行依頼受信手段が上記他の端末から端末権限認証証明書発行依頼を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、上記確認がなされた場合には上記他の端末に対して端末権限認証証明書を発行し、上記確認が拒否された場合には上記他の端末に対して端末権限認証証明書発行依頼の拒否を通知する端末権限認証証明書発行手段とをさらに具備する。これにより、端末権限認証証明書発行依頼端末を確認した上で端末権限認証証明書を発行させるという作用をもたらす。

【００１８】

また、本発明の請求項１２記載の端末は、請求項１１記載の端末において、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルをさらに具備し、上記端末権限認証証明書発行手段が、上記端末権限認証証明書の発行に際して上記端末権限認証証明書発行端末リストテーブルに保持された上記端末権限認証証明書発行端末の公開鍵証明書を上記他の端末に送信する。これにより、他の端末における端末権限認証証明書の検証を容易にするという作用をもたらす。

【００１９】

また、本発明の請求項１３記載の端末は、請求項１１記載の端末において、端末権限認証証明書の失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、上記端末権限認証証明書発行手段が、上記端末権限認証証明書の発行に際して上記端末権限認証証明書失効リストテーブルに保持された上記端末権限認証証明書失効リストを上記他の端末に送信する。これにより、他の端末において端末権限認証証明書の検証を行う際に失効している端末権限認証証明書を排除させるという作用をもたらす。

【００２０】

また、本発明の請求項１４記載の端末は、ビーコン情報を含む信号を受信するための受信手段と、この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末が端末権限認証証明書を有する旨を上記信号が示していなければ当該他の端末を所有者とする端末権限認証証明書を発行して当該他の端末に対して提案する端末権限認証証明書発行提案手段とを具備する。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に、当該信号をトリガーとして、端末権限認証証明書発行依頼に先立って端末権限認証証明書を発行させるという作用をもたらす。

【００２１】
また、本発明の請求項１５記載の端末は、請求項１４記載の端末において、上記受信手段が受信した上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、上記端末権限認証証明書発行提案手段が上記端末識別情報に基づいて上記提案を行うものである。これにより、端末権限認証証明書発行依頼を提案すべき端末を確認した上で端末権限認証証明書の受領を行わせるという作用をもたらす。
【００２２】
また、本発明の請求項１６記載の端末は、請求項１４記載の端末において、上記端末権限認証証明書発行提案手段が、上記他の端末に対して上記端末権限認証証明書発行依頼を提案する際に上記端末の公開鍵証明書を併せて提示するものである。これにより、端末権限認証証明書発行の提案をした端末の本人性をビーコン情報を含む信号の送信端末に確認させるという作用をもたらす。
【００２３】
また、本発明の請求項１７記載の端末は、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号のを送信する送信手段と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する端末権限認証証明書発行提案受信手段と、この端末権限認証証明書発行提案受信手段が他の端末から上記提案を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、上記確認がなされた場合には上記他の端末に対して端末権限認証証明書の発行を依頼し、上記確認が拒否された場合には上記他の端末に対して端末権限認証証明書発行提案の拒否を通知する端末権限認証証明書発行依頼手段とを具備する。これにより、端末権限認証証明書発行端末を確認した上で端末権限認証証明書の発行を依頼させるという作用をもたらす。
【００２４】
また、本発明の請求項１８記載の端末は、請求項１７記載の端末において、上記端末権限認証証明書発行依頼手段が、上記他の端末に対して上記端末権限認証証明書発行を依頼する際に上記端末の公開鍵証明書を併せて提示する。これにより、端末権限認証証明書発行依頼をした端末の本人性を端末権限認証証明書発行端末に確認させるという作用をもたらす。
【００２５】
また、本発明の請求項１９記載の端末は、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する送信手段と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する端末権限認証証明書発行提案受信手段と、この端末権限認証証明書発行提案受信手段が他の端末から上記提案を受信すると当該他の端末に関する情報を表示して確認を促す確認手段と、上記確認がなされると、上記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、上記提案が発行済みの端末権限認証証明書を含んでいない場合には上記他の端末に対して端末権限認証証明書の発行を依頼する端末権限認証証明書発行依頼手段とを具備する。これにより、端末権限認証証明書発行依頼の提案を受信した際にその提案が発行済みの端末権限認証証明書を含んでいるか否かを判断して、端末権限認証証明書を受領するか、端末権限認証証明書の発行を依頼するかの動作を行わせるという作用をもたらす。
【００２６】
また、本発明の請求項２０記載の端末は、請求項１９記載の端末において、上記端末権限認証証明書発行依頼手段が、上記他の端末に対して上記端末権限認証証明書発行を依頼する際に上記端末の公開鍵証明書を併せて提示するものである。これにより、端末権限認証証明書発行依頼をした端末の本人性を端末権限認証証明書発行端末に確認させるという作用をもたらす。
【００２７】
また、本発明の請求項２１記載の端末は、ビーコン情報を含む信号を受信する受信手段と、この受信手段が他の端末から所定のビーコン情報を含む信号を受信すると端末権限認証証明書発行をするよう上記他の端末に対して依頼する端末権限認証証明書発行依頼手段

とを具備する。これにより、ビーコン情報を含む信号の受信に応答して端末権限認証証明書発行の依頼を行わせるという作用をもたらす。

【００２８】

また、本発明の請求項２２記載の端末は、請求項２１記載の端末において、上記受信手段が受信した上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手段をさらに具備し、端末権限認証証明書発行依頼手段は、上記端末識別情報に基づいて上記提案を行うものである。これにより、端末権限認証証明書の発行を依頼すべき端末を確認した上で依頼を行わせるという作用をもたらす。

【００２９】

また、本発明の請求項２３記載の端末は、自端末のアクセス権限を示す第１の端末権限認証証明書を保持する端末権限認証証明書テーブルと、ビーコン情報を含む信号を受信するための受信手段と、この受信手段が他の端末からビーコン情報を含む信号を受信した場合において当該他の端末のアクセス権限を示す第２の端末権限認証証明書を当該他の端末が有する旨を上記信号が示していれば上記端末権限認証証明書テーブルに保持された上記第１の端末権限認証証明書を提示して上記他の端末に対して上記自端末の認証を要求する認証要求手段とを具備する。これにより、端末権限認証証明書を有する他の端末からのビーコン情報を含む信号をトリガーとして端末権限認証証明書に基づく相互認証処理を展開させるという作用をもたらす。

【００３０】

また、本発明の請求項２４記載の端末は、請求項２３記載の端末において、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、上記認証要求手段による認証要求に応答して上記他の端末が要求する第２の認証要求を受信する認証要求受信手段と、この認証要求受信手段が受信した上記第２の認証要求に含まれる上記第２の端末権限認証証明書を上記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段とをさらに具備する。これにより、ビーコン情報を含む信号の送信端末のアクセス権限を示す端末権限認証証明書を当該信号の受信端末に検証させるという作用をもたらす。

【００３１】

また、本発明の請求項２５記載の端末は、請求項２４記載の端末において、端末権限認証証明書失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、上記検証手段が、上記端末権限認証証明書失効リストテーブルに保持される上記端末権限認証証明書失効リストにおいて上記第２の端末権限認証証明書が失効している場合には認証失敗との判断を行う。これにより、当該端末において端末権限認証証明書の検証を行う際に失効している端末権限認証証明書を排除させるという作用をもたらす。

【００３２】

また、本発明の請求項２６記載の端末は、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、第１の端末権限認証証明書を有する他の端末に対して第２の端末権限認証証明書を有する旨を示すビーコン情報を含む信号を送信する送信手段と、自端末のアクセス権限を示す上記第２の端末権限認証証明書を保持する端末権限認証証明書テーブルと、上記信号に対する他の端末からの第１の認証要求を受信する認証要求受信手段と、この認証要求受信手段が受信した上記第１の認証要求に含まれる上記第１の端末権限認証証明書を上記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、この検証手段において認証が成功すると上記他の端末に対して上記端末権限認証証明書テーブルに保持された上記第２の端末権限認証証明書を提示して上記他の端末に対して上記自端末の認証を要求する第２の認証要求を行う認証要求手段とを具備する。これにより、端末権限認証証明書を有する旨を示すビーコン情報を含む信号をトリガーとして端末権限認証証明書に基づく相互認証処理を展開させるという作用をもたらす。

【００３３】

また、本発明の請求項２７記載の端末は、請求項２６記載の端末において、端末権限認

証証明書失効リストを保持する端末権限認証証明書失効リストテーブルをさらに具備し、上記検証手段が、上記端末権限認証証明書失効リストテーブルに保持される上記端末権限認証証明書失効リストにおいて上記第２の端末権限認証証明書が失効している場合には認証失敗との判断を行う。これにより、当該端末において端末権限認証証明書の検証を行う際に失効している端末権限認証証明書を排除させるという作用をもたらす。

【００３４】

また、本発明の請求項２８記載の端末権限認証証明書発行提案方法は、ビーコン情報を含む信号を受信する手順と、上記信号の送信元端末が端末権限認証証明書を有する旨を上記信号が示していなければ端末権限認証証明書発行依頼をするよう上記送信元端末に対して提案する手順とを具備する。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に当該信号をトリガーとして端末権限認証証明書の発行処理を展開させるという作用をもたらす。

【００３５】

また、本発明の請求項２９記載の端末権限認証証明書発行提案方法は、請求項２８記載の端末権限認証証明書発行提案方法において、上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手順をさらに具備し、上記端末識別情報に基づいて上記提案を行うものである。これにより、端末権限認証証明書発行依頼を提案すべき端末を確認した上で提案を行わせるという作用をもたらす。

【００３６】

また、本発明の請求項３０記載の端末権限認証証明書発行提案方法は、ビーコン情報を含む信号を受信する手順と、上記信号の送信元端末が端末権限認証証明書を有する旨を上記信号が示していなければ当該送信元端末を所有者とする端末権限認証証明書を発行して当該送信元端末に対して提案する手順とを具備する。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に、当該信号をトリガーとして、端末権限認証証明書発行依頼に先立って端末権限認証証明書を発行させるという作用をもたらす。

【００３７】

また、本発明の請求項３１記載の端末権限認証証明書発行依頼方法は、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、上記提案の送信元端末に関する情報を表示して確認を促す手順と、上記確認がなされた場合には上記送信元端末に対して端末権限認証証明書の発行を依頼し、上記確認が拒否された場合には上記送信元端末に対して端末権限認証証明書発行提案の拒否を通知する手順とを具備する。これにより、端末権限認証証明書発行端末を確認した上で端末権限認証証明書の発行を依頼させるという作用をもたらす。

【００３８】

また、本発明の請求項３２記載の端末権限認証証明書発行依頼方法は、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、上記提案の送信元端末に関する情報を表示して確認を促す手順と、上記確認がなされると、上記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、上記提案が発行済みの端末権限認証証明書を含んでいない場合には上記送信元端末に対して端末権限認証証明書の発行を依頼する手順とを具備する。これにより、端末権限認証証明書発行依頼の提案を受信した際にその提案が発行済みの端末権限認証証明書を含んでいるか否かを判断して、端末権限認証証明書を受領するか、端末権限認証証明書の発行を依頼するかの動作を行わせるという作用をもたらす。

【００３９】

また、本発明の請求項３３記載の端末権限認証証明書発行依頼方法は、ビーコン情報を含む信号を受信する手順と、他の端末から上記信号を受信すると端末権限認証証明書発行をするよう当該他の端末に対して依頼する手順とを具備する。これにより、ビーコン情報

を含む信号の受信に応答して端末権限認証証明書発行の依頼を行わせるという作用をもたらす。

【００４０】

また、本発明の請求項３４記載の端末権限認証証明書発行依頼方法は、本発明の請求項３３記載の端末権限認証証明書発行依頼方法において、上記他の端末からの上記信号より当該他の端末の端末識別情報を取得する手順をさらに具備し、上記端末識別情報に基づいて上記依頼を行うものである。これにより、端末権限認証証明書の発行を依頼すべき端末を確認した上で依頼を行わせるという作用をもたらす。

【００４１】

また、本発明の請求項３５記載のプログラムは、ビーコン情報を含む信号を受信する手順と、上記ビーコンの送信元端末が端末権限認証証明書を有する旨を上記信号が示していなければ端末権限認証証明書発行依頼をするよう上記送信元端末に対して提案する手順とを端末に実行させるものである。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に当該信号をトリガーとして端末権限認証証明書の発行処理を展開させるという作用をもたらす。

【００４２】

また、本発明の請求項３６記載のプログラムは、ビーコン情報を含む信号を受信する手順と、上記信号の送信元端末が端末権限認証証明書を有する旨を上記信号が示していなければ当該送信元端末を所有者とする端末権限認証証明書を発行して当該送信元端末に対して提案する手順とを端末に実行させるものである。これにより、ビーコン情報を含む信号の送信端末が端末権限認証証明書を有していない場合に、当該信号をトリガーとして、端末権限認証証明書発行依頼に先立って端末権限認証証明書を発行させるという作用をもたらす。

【００４３】

また、本発明の請求項３７記載のプログラムは、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、上記提案の送信元端末に関する情報を表示して確認を促す手順と、上記確認がなされた場合には上記送信元端末に対して端末権限認証証明書の発行を依頼し、上記確認が拒否された場合には上記送信元端末に対して端末権限認証証明書発行提案の拒否を通知する手順とを端末に実行させるものである。これにより、端末権限認証証明書発行端末を確認した上で端末権限認証証明書の発行を依頼させるという作用をもたらす。

【００４４】

また、本発明の請求項３８記載のプログラムは、端末権限認証証明書を有しない旨を示すビーコン情報を含む信号を送信する手順と、上記信号に対する端末権限認証証明書発行依頼の提案を受信する手順と、上記提案の送信元端末に関する情報を表示して確認を促す手順と、上記確認がなされると、上記提案が発行済みの端末権限認証証明書を含んでいる場合には当該端末権限認証証明書を受領し、上記提案が発行済みの端末権限認証証明書を含んでいない場合には上記送信元端末に対して端末権限認証証明書の発行を依頼する手順とを端末に実行させるものである。これにより、端末権限認証証明書発行依頼の提案を受信した際にその提案が発行済みの端末権限認証証明書を含んでいるか否かを判断して、端末権限認証証明書を受領するか、端末権限認証証明書の発行を依頼するかの動作を行わせるという作用をもたらす。

【００４５】

また、本発明の請求項３９記載のプログラムは、ビーコン情報を含む信号を受信する手順と、他の端末から上記信号を受信すると端末権限認証証明書発行をするよう当該他の端末に対して依頼する手順とを端末に実行させるものである。これにより、ビーコン情報を含む信号の受信に応答して端末権限認証証明書発行の依頼を行わせるという作用をもたらす。

【発明の効果】

【００４６】
本発明によれば、無線アドホック通信システムにおいて、端末権限認証証明書の発行を自律分散して行うことができるとという優れた効果を奏し得る。
【発明を実施するための最良の形態】
【００４７】
次に本発明の実施の形態について図面を参照して詳細に説明する。
【００４８】
図１は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末３００の構成例を示す図である。無線端末３００は、通信処理部３２０と、制御部３３０と、表示部３４０と、操作部３５０と、スピーカ３６０と、マイク３７０と、メモリ６００とを備え、これらの間をバス３８０が接続する構成となっている。また、通信処理部３２０にはアンテナ３１０が接続されている。通信処理部３２０は、アンテナ３１０を介して受信した信号からネットワークインターフェース層（データリンク層）のフレームを構成する。また、通信処理部３２０は、ネットワークインターフェース層のフレームをアンテナ３１０を介して送信する。
【００４９】
制御部３３０は、無線端末３００全体を制御する。例えば、通信処理部３２０により構成されたフレームを参照して所定の処理を行う。表示部３４０は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられ得る。操作部３５０は、無線端末３００に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられ得る。スピーカ３６０は、音声を出力するものであり、無線端末３００の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク３７０は、無線端末３００に対して外部から音声入力を行うものであり、他の端末と音声情報のやりとりを行ったり操作指示を行うために用いられる。
【００５０】
メモリ６００は、属性証明書の発行端末に関する情報を保持する属性証明書発行端末リストテーブル６１０と、無線端末３００自身のアクセス権限を示す属性証明書を保持する属性証明書テーブル６２０と、失効した属性証明書に関する情報を保持する属性証明書失効リストテーブル６３０と、無線端末３００自身の生成鍵に関する情報として公開鍵と秘密鍵と公開鍵証明書とを保持する生成鍵テーブル６５０とを格納する。
【００５１】
図２は、本発明の実施の形態における属性証明書発行端末リストテーブル６１０の構成例である。この属性証明書発行端末リストテーブル６１０は、過去に属性証明書を発行した実績のある端末に関する情報を保持するものであり、属性証明書発行端末の端末識別子６１１のそれぞれに対応して、公開鍵証明書６１２を保持している。端末識別子６１１は、ネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）におけるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス等を用いることができる。公開鍵証明書６１２は、対応する端末識別子６１１により識別される端末の公開鍵証明書である。公開鍵証明書とは、証明書所有者（サブジェクト）の本人性を証明するものであり、証明書所有者の公開鍵を含む。この公開鍵証明書は証明書発行者たる認証局（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）によって署名される。
【００５２】
図３は、属性証明書発行端末リストテーブル６１０に保持される公開鍵証明書６１２のフォーマット７１０を示す図である。この公開鍵証明書のフォーマット７１０は、大きく分けて、署名前証明書７１１と、署名アルゴリズム７１８と、署名７１９とから構成される。署名前証明書７１１は、シリアル番号７１２と、発行者７１４と、有効期限７１５と、所有者７１６と、所有者公開鍵７１７とを含む。
【００５３】
シリアル番号７１２は、公開鍵証明書のシリアル番号であり、認証局によって採番され

る。発行者７１４は、公開鍵証明書の発行者たる認証局の名前である。この発行者７１４とシリアル番号７１２とにより公開鍵証明書は一意に識別される。有効期限７１５は、公開鍵証明書の有効期限である。所有者７１６は、公開鍵証明書の所有者の名前である。所有者公開鍵７１７は、所有者７１６の公開鍵である。

【００５４】

署名７１９は公開鍵証明書に対する認証局による署名であり、署名アルゴリズム７１８はこの署名７１９のために使用された署名アルゴリズムである。署名アルゴリズムは、メッセージダイジェストアルゴリズムと公開鍵暗号アルゴリズムの２つにより構成される。メッセージダイジェストアルゴリズムは、ハッシュ関数（要約関数）の一つであり、署名前証明書７１１のメッセージダイジェストを作成するためのアルゴリズムである。ここで、メッセージダイジェストとは、入力データ（署名前証明書７１１）を固定長のビット列に圧縮したものであり、拇印や指紋（フィンガープリント）等とも呼ばれる。メッセージダイジェストアルゴリズムとしては、ＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）、ＭＤ２（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ ＃２）、ＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ ＃５）等が知られている。公開鍵暗号アルゴリズムは、メッセージダイジェストアルゴリズムにより得られたメッセージダイジェストを認証局の秘密鍵により暗号化するためのアルゴリズムである。この公開鍵暗号アルゴリズムとしては、素因数分解問題に基づくＲＳＡや離散対数問題に基づくＤＳＡ等が知られている。このように、署名前証明書７１１のメッセージダイジェストを認証局の秘密鍵により暗号化したものが署名７１９となる。

【００５５】

従って、この公開鍵証明書の署名７１９を認証局の公開鍵により復号することによってメッセージダイジェストが得られる。公開鍵証明書の利用者は、署名前証明書７１１のメッセージダイジェストを自身で作成し、それを認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前証明書７１１の内容が改ざんされていないことを検証できる。

【００５６】

図４は、属性証明書テーブル６２０に保持される属性証明書のフォーマット７２０を示す図である。この属性証明書は、大きく分けて、属性証明情報７２１と、署名アルゴリズム７２８と、署名７２９とから構成される。属性証明情報７２１は、所有者公開鍵証明書識別子７２３と、発行者７２４と、シリアル番号７２２と、有効期限７２５とを含む。

【００５７】

所有者公開鍵証明書識別子７２３は、属性証明書の所有者の公開鍵証明書を識別するためのものである。具体的には、公開鍵証明書７１０（図３）の発行者７１４とシリアル番号７１２とにより識別する。なお、この公開鍵証明書識別子７２３は、所有者を識別する機能を有するものであればよく、例えば、所有者のＭＡＣアドレスなどを利用するようにしてもよい。発行者７２４は、属性証明書の発行者たる属性認証局（ＡＡ：Ａｔｔｒｉｂｕｔｅ ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）の名称であり、例えば、発行者のＭＡＣアドレスなどを利用することができる。シリアル番号７２２は、属性証明書のシリアル番号であり、属性証明書の発行者たる属性認証局によって採番される。このシリアル番号７２２と発行者７２４とにより属性証明書は一意に識別される。有効期限７２５は、属性証明書の有効期限である。

【００５８】

署名７２９は属性証明書に対する属性認証局による署名であり、署名アルゴリズム７２８はこの署名７２９のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム７１８と同様であり、属性証明情報７２１のメッセージダイジェストを属性認証局の秘密鍵により暗号化したものが署名７２９となる。

【００５９】

従って、この属性証明書の署名７２９を属性認証局の公開鍵により復号することによっ

てメッセージダイジェストが得られる。属性証明書の利用者は、属性証明情報７２１のメッセージダイジェストを自身で作成し、それを属性認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、属性証明情報７２１の内容が改ざんされていないことを検証できる。

【００６０】

図５は、本発明の実施の形態における属性証明書失効リストテーブル６３０の構成例である。この属性証明書失効リストテーブル６３０は、失効した属性証明書に関する情報を保持するものであり、失効した属性証明書の属性証明書識別子６３１と、その失効した失効時刻６３２との対を保持している。端末を紛失した場合や盗難に遭った場合等に属性証明書を強制的に失効させるために、属性証明書失効リスト（ＡＲＬ：Ａｔｔｒｉｂｕｔｅ Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｖｏｃａｔｉｏｎ Ｌｉｓｔ）が発行される。属性証明書識別子６３１と失効時刻６３２との対は、属性証明書失効リストの各失効リストエントリから抽出されて保持される。属性証明書識別子６３１は、失効した属性証明書を識別するためのものであり、具体的には、属性証明書７２０（図４）の発行者７２４とシリアル番号７２２とにより識別する。

【００６１】

図６は、属性証明書失効リスト７３０のフォーマットを示す図である。この属性証明書失効リストは、大きく分けて、署名前失効リスト７３１と、署名アルゴリズム７３８と、署名７３９とから構成される。署名前失効リスト７３１は、署名前失効リストの発行者７３４と、０個以上の失効リストエントリ７３５とを含む。失効リストエントリ７３５は、失効した属性証明書の属性証明書識別子７３６と、その失効した失効時刻７３７との対である。この失効リストエントリ７３５における属性証明書識別子７３６と失効時刻７３７との対が、属性証明書失効リストテーブル６３０（図５）における属性証明書識別子６３１と失効時刻６３２との対に該当する。

【００６２】

署名７３９は属性証明書失効リストに対する発行者による署名であり、署名アルゴリズム７３８はこの署名７３９のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム７１８と同様であり、署名前失効リスト７３１のメッセージダイジェストを発行者の秘密鍵により暗号化したものが署名７３９となる。

【００６３】

従って、この属性証明書失効リストの署名７３９を発行者の公開鍵により復号することによってメッセージダイジェストが得られる。属性証明書失効リストの利用者は、署名前失効リスト７３１のメッセージダイジェストを自身で作成し、それを発行者の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前失効リスト７３１の内容が改ざんされていないことを検証できる。

【００６４】

なお、無線アドホック通信システムにおいては、属性証明書失効リストを集中管理する固定サーバの存在を仮定することは困難であるため、ネットワークを構成する全ての端末が属性証明書失効リストを発行し得るものとする。属性証明書失効リストを発行した端末は、他の端末に属性証明書失効リストをブロードキャスト配布することにより、他の端末においても属性証明書の有効性を検証することができる。また、ネットワークに再接続した際に、各端末が属性証明書失効リストを相互に交換し、属性証明書失効リストテーブル６３０を併合することにより最新の状態を維持する。なお、属性証明書失効リスト発行の際には、発行者を容易に認証できるよう、公開鍵証明書および属性証明書を添付することが望ましい。

【００６５】

次に本発明の実施の形態における無線アドホック通信システムの動作について図面を参照して説明する。本発明の実施の形態では、端末がネットワーク資源に接続するためには、端末が属性証明書の発行を受ける「初期登録」の手順（図７または図１５）と、端末が

属性証明書を用いて認証を行う「相互認証」の手順（図１８）とを踏むこととしている。これら図７、図１５および図１８における各処理は、無線端末３００における制御部３３０により実現される。

【００６６】

図７は、本発明の実施の形態における初期登録の手順の第１の実施例を示す図である。ここで、端末Ａ（１００）は既にネットワークに参入している属性証明書発行端末であり、端末Ｂ（２００）は新規にネットワークに参入しようとしている端末である。

【００６７】

無線アドホック通信システムにおける各端末は、他の端末に自己の存在を知らせるために定期的にビーコンを送信する。本発明の実施の形態において、ビーコンは、標識信号としてのビーコン情報のみを含む信号だけではなく、ビーコン情報に何らかのデータ情報が付加された信号をも含む。この図７の例では、端末Ｂが送信（２０１）したビーコン２０１１を端末Ａが受信し（１０１）、端末Ａが送信（１０２）したビーコン１０２２を端末Ｂが受信している（２０２）。これにより、端末Ａおよび端末Ｂは、以下のようなビーコンのフレーム構成により、互いの端末識別子を把握する。

【００６８】

これらビーコン２０１１および１０２２のフレーム構成は図８の通りである。ビーコンフレーム８１０は、ヘッダ部８１１と、ペイロード部８１２とから構成される。また、ヘッダ部８１１は、始点端末識別子８１３と、終点端末識別子８１４と、送信端末識別子８１５と、受信端末識別子８１６と、フレーム種別８１７と、属性証明書の有無８１８とを含む。始点端末識別子８１３は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、前述のようにネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）におけるＭＡＣアドレス等を用いることができる。終点端末識別子８１４は、このフレームの最終宛先の端末の端末識別子である。ビーコンフレーム８１０では、この終点端末識別子８１４にはブロードキャストアドレス（例えば、全てのビットに１）が設定される。

【００６９】

送信端末識別子８１５および受信端末識別子８１６は、フレームを中継する際に用いられる。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子８１５および受信端末識別子８１６である。

【００７０】

フレーム種別８１７は、フレームの種別を示すものであり、ここでは、ビーコンフレームであることを示す。属性証明書の有無８１８は、ネットワーク資源にアクセスする権限を示す属性証明書をビーコンフレームの送信元端末が有しているか否かを示すものである。図７の初期登録シーケンスでは、端末Ｂは属性証明書を有していないため、この属性証明書の有無８１８には「有していない」旨が示される。なお、このビーコンフレームの一例では、ペイロード部８１２のデータ８１９には他の情報は含まれない。

【００７１】

端末Ａは、端末Ｂから送信されたビーコン２０１１を受信（１０１）すると、ビーコンフレーム８１０の始点端末識別子８１４および属性証明書の有無８１８をチェックする。始点端末である端末Ｂが属性証明書を有していないと判断すると、端末Ａは属性証明書発行依頼をするよう端末Ｂに対して提案する属性証明書発行提案メッセージ１０３２を送信（１０３）する。なお、ここでは属性証明書発行提案メッセージを自動送信することを想定してビーコンに示される属性証明書の有無を検証しているが、端末Ａはこの属性証明書の有無をチェックせずに任意のタイミングで端末Ｂに対して属性証明書発行提案メッセージを作成し、送信するようにしてもよい。

【００７２】

この属性証明書発行提案メッセージ１０３２のフレーム構成は図９の通りである。属性証明書発行提案フレーム８２０は、ヘッダ部８２１と、ペイロード部８２２とから構成される。ヘッダ部８２１は、始点端末識別子８２３と、終点端末識別子８２４と、送信端末識別子８２５と、受信端末識別子８２６と、フレーム種別８２７とを含む。これらヘッダ部８２１内の内容については、図８により説明したビーコンフレーム８１０と同様である。また、この属性証明書発行提案フレーム８２０では、ペイロード部８２２のデータ８２９として、送信元である端末Ａの公開鍵証明書８２９１が含まれる。この端末Ａの公開鍵証明書８２９１は、端末Ａの生成鍵テーブル６５０に予め格納されているものである。なお、データ８２９としては、公開鍵証明書８２９１の他に端末識別子等を含んでもよい。

【００７３】

端末Ｂは、端末Ａから送信された属性証明書発行提案メッセージ１０３２を受信すると、その内容から端末Ａを確認（２０３）する。例えば、属性証明書発行提案フレーム８２０の始点端末識別子８２３（図９）や公開鍵証明書８２９１における公開鍵の所有者７１６（図３）を表示部３４０（図１）に表示することにより、正しい属性証明書発行端末であるか否かの判断をユーザに促す。これにより、アドレス偽造等による悪意のある端末や意図しない端末の介入を防ぐことができる。送信元の端末Ａが信頼する端末であり且つ端末Ａに属性証明書を発行してもらうことを意図する場合には、ユーザは操作部３５０（図１）により確認操作を行う。

【００７４】

ユーザの確認（２０３）により提案が受諾されると、端末Ｂは属性証明書発行を依頼する属性証明書発行依頼メッセージ２０４１を端末Ａに送信（２０４）する。この属性証明書発行依頼メッセージ２０４１のフレーム構成は図９の通りであり、属性証明書発行提案メッセージ１０３２のフレーム８２０と同様である。ペイロード部８３２のデータ８３９として送信元である端末Ｂの公開鍵証明書８３９１が含まれる点も同様である。

【００７５】

なお、ユーザの確認（２０３）により提案が拒否された場合には、端末Ｂは属性証明書発行提案の拒否を通知する属性証明書発行提案拒否メッセージを端末Ａに送信するようにしてもよい。この属性証明書発行提案拒否メッセージのフレーム構成は図１０の通りである。属性証明書発行提案拒否フレーム８４０は、ヘッダ部８４１と、ペイロード部８４２とから構成される。ヘッダ部８４１は、始点端末識別子８４３と、終点端末識別子８４４と、送信端末識別子８４５と、受信端末識別子８４６と、フレーム種別８４７と、拒否理由種別８４８とを含む。これらヘッダ部８４１内の内容については、図８により説明したビーコンフレーム８１０と同様であるが、拒否理由種別８４８についてはこの属性証明書発行提案拒否フレーム８４０特有のものである。この拒否理由種別８４８には、例えば、ユーザによる取り消し、属性認証局として信頼しない等の事由がコード化されて示される。

【００７６】

端末Ａは、端末Ｂから送信された属性証明書発行依頼メッセージ２０４１を受信すると、その内容から端末Ｂを確認（１０４）する。例えば、属性証明書発行依頼フレーム８３０の始点端末識別子８３３（図９）や公開鍵証明書８３９１における公開鍵の所有者７１６（図３）を表示部３４０（図１）に表示することにより、自分の信頼できる端末であるか否かの判断をユーザに促す。送信元の端末Ｂが信頼する端末であれば、ユーザは操作部３５０（図１）により確認操作を行う。

【００７７】

ユーザにより確認がなされると、端末Ａは属性証明書を発行するために属性証明書発行メッセージ１０５２を端末Ｂに送信（１０５）する。この属性証明書発行メッセージ１０５２のフレーム構成は図１１の通りである。属性証明書発行フレーム８６０は、ヘッダ部８６１と、ペイロード部８６２とから構成される。ヘッダ部８６１は、始点端末識別子８６３と、終点端末識別子８６４と、送信端末識別子８６５と、受信端末識別子８６６と、フレーム種別８６７とを含む。これらヘッダ部８６１内の内容については、図９により説

明した属性証明書発行提案フレーム８２０と同様である。また、この属性証明書発行フレーム８６０では、ペイロード部８６２のデータ８６９として、依頼元である端末Ｂを所有者として端末Ａにより署名された属性証明書８６９１が含まれる。端末Ａから属性証明書発行メッセージ１０５２を受信（２０５）した端末Ｂは、属性証明書発行フレーム８６０から属性証明書８６９１を抽出して、属性証明書テーブル６２０に格納する。

【００７８】

なお、ユーザにより確認（１０４）が拒否された場合には、端末Ａは属性証明書発行依頼の拒否を通知する属性証明書発行依頼拒否メッセージを端末Ｂに送信するようにしてもよい。この属性証明書発行依頼拒否メッセージのフレーム構成は図１０の通りであり、属性証明書発行提案拒否フレーム８４０と同様である。

【００７９】

図１２は、本発明の実施の形態における初期登録手順の第１の実施例の変形例を示す図である。この変形例では、属性証明書発行端末から属性証明書発行提案メッセージを送信する際に、属性証明書を発行してそのメッセージに添付しておくことにより、端末間でやりとりされるメッセージの数を減らすものである。ここで、端末Ａ（１００）が属性証明書発行端末であり、端末Ｂ（２００）が新規参入端末である点は、図７の第１の実施例と同様である。両端末がビーコンを送信し合う点も同様であり、端末Ｂが送信（２３１）したビーコン２３１１を端末Ａが受信（１３１）し、端末Ａが送信したビーコン１３２２を端末Ｂが受信（２３２）することにより、端末Ａおよび端末Ｂは互いの端末識別子を把握する。これらビーコンのフレーム構成も第１の実施例と同様に図８で説明した通りである。

【００８０】

この図１２の実施例では、図７の第１の実施例とは異なり、ビーコンを受信した属性証明書発行端末である端末Ａ（１００）が、属性証明書発行依頼メッセージ（図７の２０４１）を受けることなく新規参入端末である端末Ｂ（２００）に対して属性証明書を発行し、属性証明書発行提案メッセージ１３３２のペイロード部のデータに含めて送信する。この属性証明書には、発行先である端末Ｂを所有者として端末Ａによる署名がなされる。この場合の属性証明書発行提案メッセージ１３３２のフレーム構成１８２０は図１３の通りであり、ペイロード部１８２２のデータ１８２９として発行先端末への属性証明書１８２９２を含んでいる点を除いて図９の属性証明書発行提案メッセージのフレーム構成８２０と同様の構成となっている。これにより、図７の第１の実施例と比べてメッセージ数を減らすことが可能となる。なお、属性証明書発行提案メッセージが属性証明書１８２９２を含むか否かは、端末Ｂ（２００）においてフレーム種別８２７または１８２７により判断するようにしてもよく、また、別途フィールドを設けてそのフィールドの内容により判断するようにしてもよい。

【００８１】

図１２の実施例では、端末Ｂ（２００）は、端末Ａ（１００）から送信（１３３）された属性証明書発行提案メッセージ１３３２を受信（２３３）すると、その内容から端末Ａ（１００）を確認する。例えば、属性証明書発行提案フレーム１８２０の始点端末識別子１８２３を表示することにより、正しい属性証明書発行端末であるか否かの判断をユーザに促す。これにより、アドレス偽造等による悪意のある端末や意図しない端末の介入を防ぐことができる。送信元の端末Ａ（１００）が信頼する端末であり且つ端末Ａ（１００）が発行した属性証明書を受け入れる場合には、ユーザは操作部３５０（図１）により確認操作を行う。端末Ａ（１００）からの属性証明書発行提案メッセージ１３３２を受け入れた端末Ｂ（２００）は、属性証明書発行提案フレーム１８２０のペイロード部１８２２から属性証明書１８２９２を抽出して、属性証明書テーブル６２０（図１）に格納する。

【００８２】

ユーザにより確認（２３３）がなされると、端末Ｂ（２００）は属性証明書発行提案メッセージ１３３２を受領する属性証明書発行提案受領メッセージ２３４１を端末Ａ（１００）に送信（２３４）する。この属性証明書発行提案受領メッセージ２３４１のフレーム

構成１８３０は図１４の通りであり、基本的には図９の属性証明書発行依頼メッセージのフレーム構成と同様の構成になっている。

【００８３】

なお、ユーザの確認（２３３）により提案が拒否された場合には、端末Ｂ（２００）は属性証明書発行提案の拒否を通知する属性証明書発行提案拒否メッセージを端末Ａに送信するようにしてもよい。この属性証明書発行提案拒否メッセージのフレーム構成８４０は図１０で説明したものと同様の構成である。

【００８４】

図１５は、本発明の実施の形態における初期登録の手順の第２の実施例を示す図である。端末Ａ（１００）が属性証明書発行端末であり、端末Ｂ（２００）が新規参入端末である点は、図７の第１の実施例と同様である。両端末がビーコンを送信し合う点も同様であり、端末Ｂが送信（２２１）したビーコン２２１１を端末Ａが受信し（１２１）、端末Ａが送信（１２２）したビーコン１２２２を端末Ｂが受信（２２２）することにより、端末Ａおよび端末Ｂは互いの端末識別子を把握する。これらビーコン２２１１および１２２２のフレーム構成も同様に図８の通りである。

【００８５】

この図１５の第２の実施例では、図７の第１の実施例とは異なり、ビーコンを受信した新規参入端末である端末Ｂが、属性証明書発行提案メッセージを受けることなく、属性証明書発行端末である端末Ａに対して属性証明書発行依頼メッセージ２２５１を送信（２２５）する。この属性証明書発行依頼メッセージ２０４１のフレーム構成８３０は図９により説明した通りである。この際、もしも属性証明書発行依頼メッセージ２２５１の送信先である端末Ａの公開鍵証明書を端末Ｂが有していない場合には、端末Ｂは公開鍵証明書要求メッセージ２２３１を送信することにより公開鍵証明書を端末Ａに要求する（２２３）。この公開鍵証明書要求メッセージ２２３１のフレーム構成１８７０は図１６の通りであり、図７の第１の実施例において説明した属性証明書発行提案メッセージ１０３２のフレーム８２０（図９）と同様である。但し、ペイロード部１８７２には公開鍵証明書は含まれない。

【００８６】

公開鍵証明書要求メッセージ２２３１を受信（１２３）した端末Ａは、生成鍵テーブル６５０（図１）に保持している自端末の公開鍵証明書を公開鍵証明書要求応答メッセージ１２４２により送信（１２４）する。これにより、端末Ｂは属性証明書発行端末である端末Ａの公開鍵証明書を受領（２２４）する。なお、この公開鍵証明書要求応答メッセージ１２４２のフレーム構成１８８０は図１７の通りであり、図７の第１の実施例において説明した属性証明書発行提案メッセージ１０３２のフレーム８２０（図９）と同様である。ペイロード部１８８２のデータとして送信元端末である端末Ａの公開鍵証明書１８８９が含まれる点も同様である。

【００８７】

端末Ａは、端末Ｂから送信された属性証明書発行依頼メッセージ２２５１を受信すると、その内容から端末Ｂを確認（１２５）する。例えば、属性証明書発行依頼フレーム８３０の始点端末識別子８３３（図９）や公開鍵証明書８３９１における公開鍵の所有者７１６（図３）を表示部３４０（図１）に表示することにより、自分の信頼できる端末であるか否かの判断をユーザに促す。送信元の端末Ｂが信頼する端末であれば、ユーザは操作部３５０（図１）により確認操作を行う。

【００８８】

ユーザにより確認がなされると、端末Ａは属性証明書を発行するために属性証明書発行メッセージ１２６２を端末Ｂに送信（１２６）する。これにより、端末Ｂは属性証明書を受領（２２６）する。なお、この属性証明書発行メッセージ１２６２のフレーム構成８６０は図１１により説明した通りである。

【００８９】

図１８は、本発明の実施の形態における相互認証の手順を示す図である。初期登録を終

えた端末同士が互いの属性証明書を検証することにより相互認証を行う。本発明の実施の形態における無線アドホック通信システムでは、各端末は定期的にビーコンを送信し、他の端末に対して自己の存在を知らせる。以下では、端末Bのビーコンをトリガーとして端末Aが認証要求を行うものと仮定するが、最終的に相互に認証が行われればよく、何れの端末のビーコンをトリガーとしてもよい。

【００９０】

まず、端末Bが、ネットワークに参入するためにビーコン２１１１を送信する（２１１）。このビーコン２１１１のフレーム構成は上述の図８の通りである。図７の初期登録シーケンスと異なり、この図１８の相互認証においては端末Bは属性証明書を有しているため、この属性証明書の有無８１８には「有している」旨が示される。

【００９１】

端末Aは、端末Bから送信されたビーコン２１１１を受信すると（１１１）、ビーコンフレーム８１０の属性証明書の有無８１８をチェックする。端末Bが属性証明書を有していると判断すると、端末Aは端末Bに対して端末Aを認証するよう認証要求メッセージ１１２２を送信する（１１２）。この認証要求メッセージ１１２２のフレーム構成は図１９の通りである。認証要求フレーム８７０は、ヘッダ部８７１と、ペイロード部８７２とから構成される。ヘッダ部８７１は、始点端末識別子８７３と、終点端末識別子８７４と、送信端末識別子８７５と、受信端末識別子８７６と、フレーム種別８７７とを含む。これらヘッダ部８７１内の内容については、図９により説明した属性証明書発行提案フレーム８２０と同様である。また、この認証要求フレーム８７０では、ペイロード部８７２のデータ８７９として、送信元である端末Aの公開鍵証明書８７９１および属性証明書８７９２が含まれる。端末Aの公開鍵証明書８７９１は端末Aの生成鍵テーブル６５０に予め格納されたものであり、端末Aの属性証明書８７９２は端末Aの属性証明書テーブル６２０に予め格納されたものである。

【００９２】

端末Bは、端末Aから送信された認証要求メッセージ１１２２を受信すると、その内容から端末Aを認証する（２１２）。具体的には、属性証明書発行端末リストテーブル６１０の公開鍵証明書６１２（図２）から属性認証局の公開鍵を抽出して、この公開鍵によって認証要求メッセージ１１２２に含まれる属性証明書８７９２の署名７２９（図４）を復号することにより署名時のメッセージダイジェストを得る。そして、属性証明書８７９２の属性証明情報７２１（図４）のメッセージダイジェストを新たに生成する。この新たに生成されたメッセージダイジェストが署名時のメッセージダイジェストと一致していることを確認する。もしこれらが一致しないとすれば、属性証明書は署名後に改ざんされた可能性があり、属性証明書の検証は失敗となる。両者が一致している場合には、さらに認証要求メッセージ１１２２に含まれる属性証明書８７９２の所有者公開鍵証明書識別子７２３（図４）が、認証要求メッセージ１１２２に含まれる公開鍵証明書８７９１の発行者７１４およびシリアル番号７１２（図３）に一致することを確認する。これが一致すれば、公開鍵証明書の所有者である端末Aは属性証明書の所有者であることが確認できる。もしこれらが一致しないとすれば、属性証明書の所有者は端末Aではなく、属性証明書の検証は失敗となる。

【００９３】

なお、この属性証明書の検証の際には、その属性証明書が属性証明書失効リストテーブル６３０に含まれていないことを確認する必要がある。属性証明書８７９２の発行者７２４およびシリアル番号７２２（図４）が属性証明書失効リストテーブル６３０の属性証明書識別子６３１（図５）に含まれている場合には、その属性証明書８７９２は失効時刻６３２を境に失効していることになる。従って、その場合には属性証明書の検証は失敗となる。

【００９４】

端末Aの認証（２１２）に成功すると、端末Bは端末Aの認証に成功したことを通知する認証成功メッセージ２１３１を端末Aに送信する（２１３）。この認証成功メッセージ

２１３１の認証応答フレーム構成は図２０の通りである。認証応答フレーム８８０は、ヘッダ部８８１と、ペイロード部８８２とから構成される。ヘッダ部８８１は、始点端末識別子８８３と、終点端末識別子８８４と、送信端末識別子８８５と、受信端末識別子８８６と、フレーム種別８８７とを含む。これらヘッダ部８８１内の内容については、図９により説明した属性証明書発行提案フレーム８２０と同様である。認証成功メッセージ２１３１の場合、フレーム種別８８７は認証成功フレームとなる。この認証応答フレーム８８０では、さらに応答理由種別８８８を含むが、認証成功の場合は特に必要はない。

【００９５】

なお、端末Ａの属性証明書の検証（２１２）に失敗すると、端末Ｂは端末Ａの認証に成功したことを通知する認証失敗メッセージを端末Ａに送信することになる。この認証失敗メッセージの認証応答フレーム構成は図２０により説明した通りである。但し、認証失敗メッセージの場合、フレーム種別８８７は認証失敗フレームとなり、応答理由種別８８８には認証に失敗した理由として属性証明書のメッセージダイジェスト不一致、属性証明書失効等の事由がコード化されて示される。これら。認証成功メッセージ２１３１または認証失敗メッセージは端末Ａにおいて受信されて確認される（１１３）。

【００９６】

端末Ａの属性証明書の検証（２１２）に成功すると、さらに端末Ｂは端末Ａに対して端末Ｂを認証するよう認証要求メッセージ２１４１を送信する（２１４）。この認証要求メッセージ２１４１のフレーム構成は上述の図１９と同様であり、送信元である端末Ｂの公開鍵証明書８７９１および属性証明書８７９２が含まれる。

【００９７】

端末Ａは、端末Ｂから送信された認証要求メッセージ２１４１を受信すると、その内容から端末Ｂを認証する（１１４）。この認証の内容は既に説明した通りであり、属性証明書の検証、属性証明書の所有者の確認、および、属性証明書失効リストテーブル６３０の確認等を行う。

【００９８】

端末Ｂの認証（２１２）に成功すると、端末Ａは端末Ｂの認証に成功したことを通知する認証成功メッセージ１１５２を端末Ｂに送信する（１１５）。この認証成功メッセージ１１５２の認証応答フレーム構成は上述の図２０と同様である。また、端末Ｂの属性証明書の検証（２１２）に失敗した場合には、端末Ａは端末Ｂの認証に成功したことを通知する認証失敗メッセージを端末Ｂに送信することになる。この認証失敗メッセージの認証応答フレーム構成も図２０により説明した通りである。これら認証成功メッセージ１１５２または認証失敗メッセージは端末Ｂにおいて受信されて確認される（２１５）。

【００９９】

このようにして、端末Ａおよび端末Ｂにおいて互いの端末の認証に成功すると相互認証は完了する。この相互認証が完了した後、属性証明書発行端末リストテーブル６１０および属性証明書失効リストテーブル６３０の内容を相互に交換して併合する。また、新たに属性証明書発行端末になった端末は、自己の公開鍵証明書を全ての端末にブロードキャスト配布する。さらに、上述のように、属性証明書失効リストを発行した端末は、他の端末に属性証明書失効リストをブロードキャスト配布する。これらにより、ネットワークに接続中の各端末の属性証明書発行端末リストテーブル６１０および属性証明書失効リストテーブル６３０の内容の同一性が維持される。

【０１００】

次に本発明の実施の形態における無線アドホック通信システムの各端末の処理の流れについて図面を参照して説明する。

【０１０１】

図２１は、図７の初期登録の第１の実施例における属性証明書発行端末の処理の流れを示す図である。まず、他の端末からビーコンを受信すると、そのビーコンの送信元端末が属性証明書を有している旨をそのビーコンが示しているか否かを判断する（ステップＳ９１１）。属性証明書を有している旨をそのビーコンが示していれば、属性証明書を発行す

る必要がないので、この初期登録の処理は行わずに終了する。属性証明書を有している旨をそのビーコンが示していなければ、ビーコンの始点端末識別子を確認して、送信元端末に対して属性証明書の発行を依頼することを提案する（ステップＳ９１２）。

【０１０２】

その後、属性証明書の発行依頼があれば（ステップＳ９１３）、その依頼元端末に関する情報を表示して確認を促す（ステップＳ９１４）。その結果、依頼元端末が信頼できる端末として確認された場合には（ステップＳ９１５）、依頼元端末に対して属性証明書を発行する（ステップＳ９１６）。逆に、確認が拒否された場合には依頼元端末に対して属性証明書発行依頼の拒否を通知する（ステップＳ９１７）。

【０１０３】

図２２は、図７の初期登録の第１の実施例における新規参入端末の処理の流れを示す図である。まず、属性証明書を有していない旨を示すビーコンを送信する（ステップＳ９２１）。その後、ビーコンに応答した他の端末からの属性証明書発行提案があると（ステップＳ９２２）、その提案をした端末の確認をユーザに促す（ステップＳ９２３）。送信元の端末が信頼する端末であればその端末に属性証明書を発行してもらうことを意図する確認がなされる（ステップＳ９２４）。この確認がなされるとその送信元端末に対して属性証明書の発行依頼を行う（ステップＳ９２５）。これにより、属性証明書の発行を受けることができる（ステップＳ９２６）。一方、この確認がされなければ初期登録の処理は完了せず、属性証明書は発行されない。

【０１０４】

図２３は、図１２の初期登録の第１の実施例の変形例における属性証明書発行端末の処理の流れを示す図である。まず、他の端末からビーコンを受信すると、そのビーコンの送信元端末が属性証明書を有している旨をそのビーコンが示しているか否かを判断する（ステップＳ９７１）。属性証明書を有している旨をそのビーコンが示していれば、属性証明書を発行する必要がないので、この初期登録の処理は行わずに終了する。属性証明書を有している旨をそのビーコンが示していなければ、ビーコンの始点端末識別子を確認して、送信元端末に対して属性証明書を発行し（ステップＳ９７２）、その属性証明書を提案メッセージに含めて送信する（ステップＳ９７３）。

【０１０５】

図２４は、図１２の初期登録の第１の実施例の変形例における新規参入端末の処理の流れを示す図である。まず、属性証明書を有していない旨を示すビーコンを送信する（ステップＳ９８１）。その後、ビーコンに応答した他の端末からの属性証明書発行提案があると（ステップＳ９８２）、その提案をした端末の確認（ステップＳ９８３）をユーザに促す。送信元の端末が信頼する端末であれば（ステップＳ９８４）、その端末が発行した属性証明書を受領して（ステップＳ９８５）、その属性証明書を受領した旨を示すメッセージを送信元の端末に送信する（ステップＳ９８６）。

【０１０６】

図２５は、図１５の初期登録の第２の実施例における新規参入端末の処理の流れを示す図である。まず、受信したビーコンの始点端末識別子８１３（図８）を把握し、そのビーコンの送信元端末に属性証明書の発行を依頼するか否かを判断する（ステップＳ９５１）。発行を希望しない場合には、当該処理は終了する。もし、新規参入端末がビーコン送信元端末の公開鍵証明書を所持していない場合には（ステップＳ９５２）、ビーコン送信元端末に対して公開鍵証明書を要求し（ステップＳ９５３）、受領する（ステップＳ９５４）。

【０１０７】

そして、公開鍵証明書に含まれる公開鍵がビーコン送信元端末のものであって、当該端末に属性証明書を発行してもらうと判断した場合には（ステップＳ９５５）、その送信元端末に対して属性証明書の発行依頼を行う（ステップＳ９５６）。これにより、属性証明書の発行を受けることができる。一方、公開鍵がビーコン送信元端末のものであることが確認できない場合には、属性証明書の発行依頼は行わない。

【０１０８】

図２６は、図１５の初期登録の第２の実施例における属性証明書発行端末の処理の流れを示す図である。まず、他の端末から公開鍵証明書の要求があれば（ステップＳ９６１）、要求に応答して公開鍵証明書を送信する（ステップＳ９６２）。その後、属性証明書の発行依頼があれば（ステップＳ９６３）、その依頼元端末に関する情報を表示して確認を促す（ステップＳ９６４）。その結果、依頼元端末が信頼できる端末として確認された場合には（ステップＳ９６５）、依頼元端末に対して属性証明書を発行する（ステップＳ９６６）。逆に、確認が拒否された場合には依頼元端末に対して属性証明書発行依頼の拒否を通知する（ステップＳ９６７）。

【０１０９】

図２７は、図１８の相互認証におけるビーコン受信端末の処理の流れを示す図である。まず、他の端末からビーコンを受信すると、そのビーコンの送信端末が属性証明書を有している旨をそのビーコンが示しているか否かを判断する（ステップＳ９３１）。属性証明書を有している旨をそのビーコンが示していなければ、相互認証を行うことができないため、この相互認証の処理は行わずに終了する。なお、この場合には属性証明書発行端末から属性証明書発行の提案がなされる。一方、属性証明書を有している旨をそのビーコンが示していれば、ビーコンの送信端末に対して認証要求を送信する（ステップＳ９３２）。この結果、ビーコンの送信端末において認証が失敗すると、この相互認証は完了せず（ステップＳ９３３）、両端末は互いにネットワークを構成することができない。一方、ビーコンの送信端末において認証が成功すると、反対にビーコン送信端末から認証要求が送信される。

【０１１０】

認証要求を受信すると（ステップＳ９３４）、認証要求元のビーコン送信端末の認証を行う（ステップＳ９３５）。認証に成功すれば（ステップＳ９３６）、認証成功の旨を認証要求端末（ビーコン送信端末）に送信する（ステップＳ９３７）。一方、認証に失敗した場合には（ステップＳ９３６）、認証失敗の旨を認証要求端末に送信する（ステップＳ９３８）。

【０１１１】

図２８は、図１８の相互認証におけるビーコン送信端末の処理の流れを示す図である。まず、属性証明書を有している旨を示すビーコンを送信する（ステップＳ９４１）。その後、ビーコンに応答した他の端末からの認証要求を受信すると（ステップＳ９４２）、認証要求元のビーコン受信端末の認証を行う（ステップＳ９４３）。認証に失敗した場合には（ステップＳ９４４）、認証失敗の旨を認証要求端末（ビーコン受信端末）に送信する（ステップＳ９４５）。一方、認証に成功した場合には（ステップＳ９４４）、認証成功の旨を認証要求端末に送信するとともに（ステップＳ９４６）、ビーコン受信端末に対して認証要求を送信する（ステップＳ９４７）。その後、ビーコン受信端末から認証要求に対する応答が送信される（ステップＳ９４８）。

【０１１２】

次に本発明の実施の形態における無線アドホック通信システムの端末間の接続関係について図面を参照して説明する。

【０１１３】

図２９は、端末同士が無線アドホック通信システムのネットワークを構成していく過程を示す図である。最初に端末Ａ（１００）が属性証明書発行端末として機能しているとすると、端末Ａの属性証明書発行端末リストテーブル６１０には端末Ａの公開鍵証明書（ＰＫ－Ａ）が保持され、端末Ａの属性証明書テーブルには端末Ａ発行の属性証明書（ＡＣ－Ａ）が保持される（図２９（ａ））。端末Ｂ（２００）がビーコンを送信すると、端末Ａから端末Ｂに対して属性証明書が発行され、初期登録の結果、端末Ｂの属性証明書発行端末リストテーブル６１０には端末Ａの公開鍵証明書（ＰＫ－Ａ）が保持され、端末Ｂの属性証明書テーブルには端末Ａ発行の属性証明書（ＡＣ－Ａ）が保持される（図２９（ｂ））。初期登録の後、相互認証が行われることにより、端末Ａと端末Ｂは無線アドホック通

信システムのネットワークを構成する。

【０１１４】

その後、端末Ｃがビーコンを送信すると、端末Ｂを介して端末Ａから端末Ｃに対して属性証明書が発行され、初期登録の後、例えば端末Ｂと相互認証を行うことにより端末Ｃは無線アドホック通信システムのネットワークに参入する（図２９（ｃ））。さらに、端末Ｃがビーコンを送信した場合も同様の手順を経て、端末Ｄは無線アドホック通信システムのネットワークに参入する（図２９（ｃ））。

【０１１５】

そして、これまで属性証明書発行端末として機能していた端末Ａが何らかの要因によりネットワークから切断されると、他の端末が属性証明書発行端末として機能することになる。この属性証明書発行端末の選択基準としては種々のものが考えられるが、例えば、ある時点で中心位置に存在している端末や、電池の残容量が最も多い端末等を選択することができる。例えば、端末Ｂが属性証明書発行端末として選択されたとすると、端末Ｂは自己の公開鍵証明書（ＰＫ－Ｂ）を接続中の全端末にブロードキャスト配布する。各端末は、端末Ｂの公開鍵証明書（ＰＫ－Ｂ）を端末Ｂの端末識別子とともに属性証明書発行端末リストテーブル６１０に格納する（図２９（ｄ））。

【０１１６】

図３０は、一旦切断された端末が無線アドホック通信システムのネットワークに再び参入する過程を示す図である。端末Ａが切断されて端末Ｂが属性証明書発行端末として機能するようになった後に、端末Ｅがビーコンを送信すると（図３０（ａ））、端末Ｂから端末Ｅに対して属性証明書が発行される。初期登録の結果、端末Ｅの属性証明書発行端末リストテーブル６１０には現行の属性証明書発行端末である端末Ｂの公開鍵証明書（ＰＫ－Ｂ）と過去の属性証明書発行端末である端末Ａの公開鍵証明書（ＰＫ－Ａ）が保持される。また、端末Ｅの属性証明書テーブルには端末Ｂ発行の属性証明書（ＡＣ－Ｂ）が保持される（図３０（ｂ））。

【０１１７】

その後、端末Ａが再び接続する場合には、端末Ａは保持していた端末Ａ発行による属性証明書（ＡＣ－Ａ）により認証を行う。そして、相互認証後、端末Ｂとの間で属性証明書発行端末リストテーブル６１０の更新を行う。その結果、端末Ａの属性証明書発行端末リストテーブル６１０には新たに端末Ｂの公開鍵証明書（ＰＫ－Ｂ）が保持される（図３０（ｃ））。

【０１１８】

このように、本発明の実施の形態によれば、ビーコンを受信した属性証明書発行端末がビーコンフレーム８１０の属性証明書の有無８１８（図８）をチェックして、ビーコン送信端末が属性証明書を有していないと判断した場合には、属性証明書の発行依頼を提案する属性証明書発行提案フレーム８２０（図９）をビーコン送信端末に対して送信することにより、これらを契機として属性証明書を自律分散して発行することができる。

【０１１９】

なお、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

【０１２０】

また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータ（端末）に実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

【産業上の利用可能性】

【０１２１】

本発明の活用例として、例えば無線アドホック通信システムにおける端末間において端末権限認証証明書の発行を行う際に本発明を適用することができる。

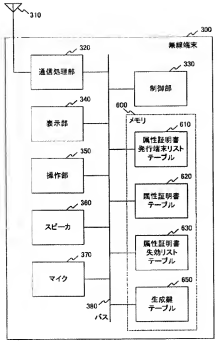
【図面の簡単な説明】

【０１２２】

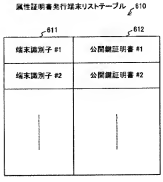
【図１】本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末３００の構成例を示す図である。
【図２】本発明の実施の形態における属性証明書発行端末リストテーブル６１０の構成例である。
【図３】本発明の実施の形態における属性証明書発行端末リストテーブル６１０に保持される公開鍵証明書６１２のフォーマット７１０を示す図である。
【図４】本発明の実施の形態における属性証明書テーブル６２０に保持される属性証明書のフォーマット７２０を示す図である。
【図５】本発明の実施の形態における属性証明書失効リストテーブル６３０の構成例である。
【図６】本発明の実施の形態における属性証明書失効リスト７３０のフォーマットを示す図である。
【図７】本発明の実施の形態における初期登録の手順の第１の実施例を示す図である。
【図８】本発明の実施の形態におけるビーコンフレーム８１０の構成を示す図である。
【図９】本発明の実施の形態における属性証明書発行提案フレーム８２０および属性証明書発行依頼フレーム８３０の構成を示す図である。
【図１０】本発明の実施の形態における属性証明書発行提案拒否フレーム８４０および属性証明書発行依頼拒否フレーム８５０の構成を示す図である。
【図１１】本発明の実施の形態における属性証明書発行フレーム８６０の構成を示す図である。
【図１２】本発明の実施の形態における初期登録の手順の第１の実施例の変形例を示す図である。
【図１３】本発明の実施の形態における属性証明書発行提案フレーム１８２０の構成を示す図である。
【図１４】本発明の実施の形態における属性証明書発行提案受領フレーム１８３０の構成を示す図である。
【図１５】本発明の実施の形態における初期登録の手順の第２の実施例を示す図である。
【図１６】本発明の実施の形態における公開鍵証明書要求フレーム８７０の構成を示す図である。
【図１７】本発明の実施の形態における公開鍵証明書要求応答フレーム８８０の構成を示す図である。
【図１８】本発明の実施の形態における相互認証の手順を示す図である。
【図１９】本発明の実施の形態における認証要求フレーム８７０の構成を示す図である。
【図２０】本発明の実施の形態における認証応答フレーム８８０の構成を示す図である。
【図２１】本発明の実施の形態における初期登録の際の属性証明書発行端末の第１の実施例における処理の流れを示す図である。
【図２２】本発明の実施の形態における初期登録の際の新規参入端末の第１の実施例における処理の流れを示す図である。
【図２３】本発明の実施の形態における初期登録の際の属性証明書発行端末の第１の実施例の変形例における処理の流れを示す図である。
【図２４】本発明の実施の形態における初期登録の際の新規参入端末の第１の実施例の変形例における処理の流れを示す図である。
【図２５】本発明の実施の形態における初期登録の際の新規参入端末の第２の実施例における処理の流れを示す図である。
【図２６】本発明の実施の形態における初期登録の際の属性証明書発行端末の第２の実施例における処理の流れを示す図である。
【図２７】本発明の実施の形態における相互認証の際のビーコン受信端末の処理の流れを示す図である。
【図２８】本発明の実施の形態における相互認証の際のビーコン送信端末の処理の流れを示す図である。

【図２９】本発明の実施の形態において端末同士が無線アドホック通信システムのネットワークを構成していく過程を示す図である。
【図３０】本発明の実施の形態において一旦切断された端末が無線アドホック通信システムのネットワークに再び参入する過程を示す図である。
【符号の説明】
【０１２３】
３００　無線端末
３１０　アンテナ
３２０　通信処理部
３３０　制御部
３４０　表示部
３５０　操作部
３６０　スピーカ
３７０　マイク
３８０　バス
６００　メモリ
６１０　属性証明書発行端末リストテーブル
６２０　属性証明書テーブル
６３０　属性証明書失効リストテーブル
６５０　生成鍵テーブル
７１０　公開鍵証明書
７２０　属性証明書
７３０　属性証明書失効リスト
８１０　ビーコンフレーム
８２０　属性証明書発行提案フレーム
８３０　属性証明書発行依頼フレーム
８４０　属性証明書発行提案拒否フレーム
８５０　属性証明書発行依頼拒否フレーム
８６０　属性証明書発行フレーム
８７０　認証要求フレーム
８８０　認証応答フレーム
１８２０　属性証明書発行提案フレーム
１８３０　属性証明書発行提案受領フレーム
１８７０　公開鍵証明書要求フレーム
１８８０　公開鍵証明書要求応答フレーム

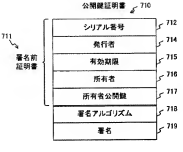
【図１】


310
300
無線端末
320
通信処理部
330
制御部
340
表示部
600
メモリ
610
属性証明書発行端末リストテーブル
350
操作部
620
属性証明書テーブル
360
スピーカ
630
属性証明書失効リストテーブル
370
マイク
650
生成鍵テーブル
380
バス

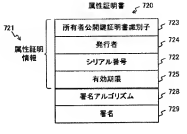
【図２】


属性証明書発行端末リストテーブル
610
611
612
端末識別子 #1
公開鍵証明書 #1
端末識別子 #2
公開鍵証明書 #2

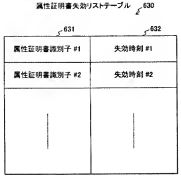
【図３】


公開鍵証明書
710
711
署名前証明書
シリアル番号
712
発行者
714
有効期限
715
所有者
716
所有者公開鍵
717
署名アルゴリズム
718
署名
719

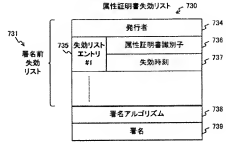
【図４】


属性証明書
720
721
属性証明情報
所有者公開鍵証明書識別子
723
発行者
724
シリアル番号
722
有効期限
725
署名アルゴリズム
728
署名
729

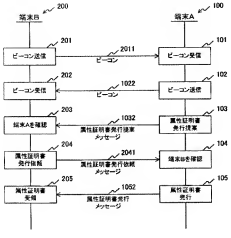
【図５】


属性証明書失効リストテーブル
630
631
632
属性証明書識別子 #1
失効時刻 #1
属性証明書識別子 #2
失効時刻 #2

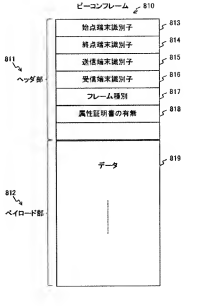
【図６】


属性証明書失効リスト
730
731
署名前失効リスト
735
失効リストエントリ #1
734
発行者
736
属性証明書識別子
737
失効時刻
738
署名アルゴリズム
739
署名

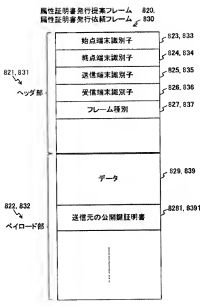
【図７】


200
端末B
100
端末A
201
ビーコン送信
2011
ビーコン
101
ビーコン受信
202
ビーコン受信
1022
ビーコン
102
ビーコン送信
203
端末Aを確認
1032
属性証明書発行要求メッセージ
103
属性証明書発行要求
204
属性証明書発行後報
2041
属性証明書発行後報メッセージ
104
端末Bを確認
205
属性証明書受信
1052
属性証明書完了メッセージ
105
属性証明書完了

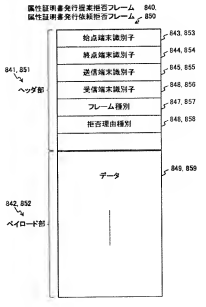
【図８】


ビーコンフレーム
810
811
ヘッダ部
813
始点端末識別子
814
終点端末識別子
815
送信端末識別子
816
受信端末識別子
817
フレーム種別
818
属性証明書の有無
819
データ
812
ペイロード部

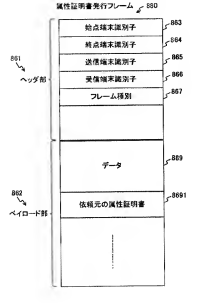
【図９】



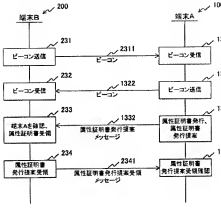
【図１０】



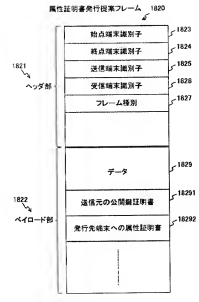
【図１１】



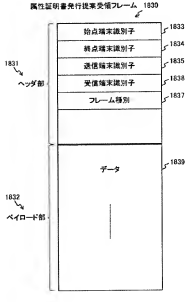
【図１２】



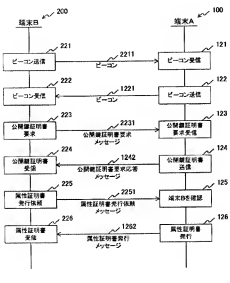
【図１３】



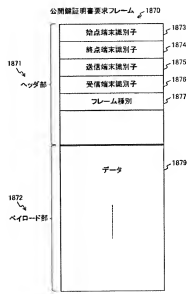
【図１４】



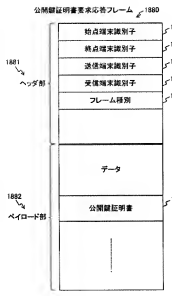
【図１５】



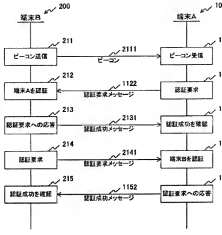
【図１６】



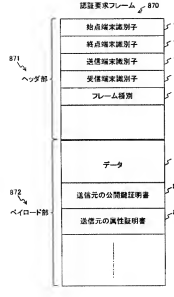
【図１７】



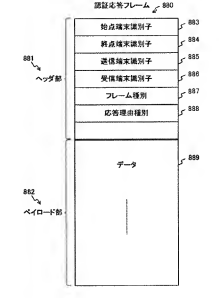
【図１８】



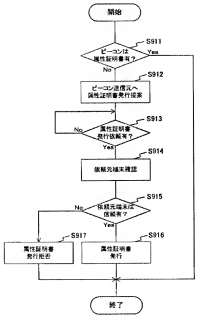
【図１９】



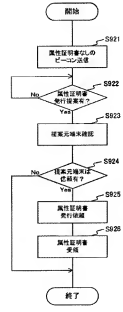
【図２０】



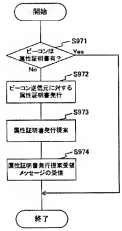
【図２１】



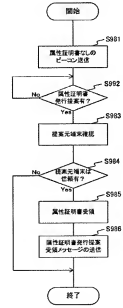
【図２２】



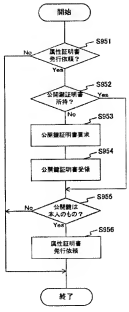
【図２３】



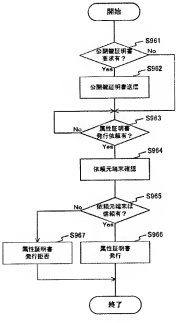
【図２４】



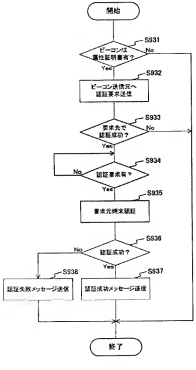
【図２５】



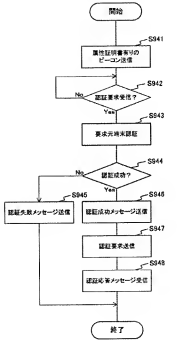
【図２６】



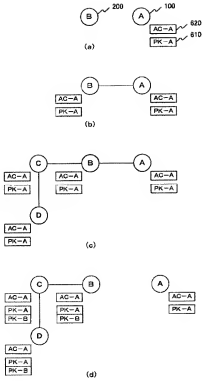
【図２７】



【図２８】



【図２９】



【図３０】